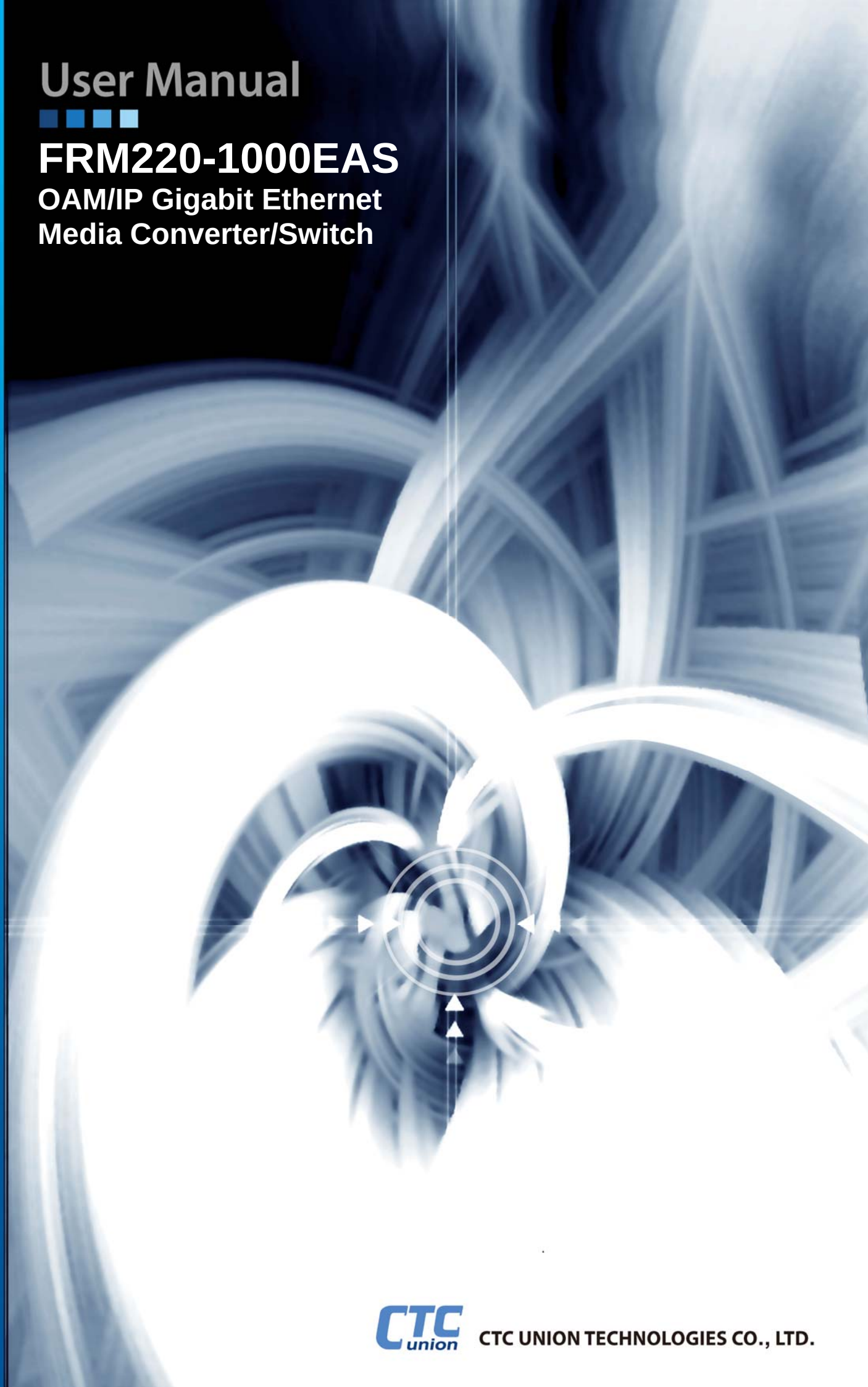
User Manual

FRM220-1000EAS

OAM/IP Gigabit Ethernet Media Converter/Switch



CTC UNION TECHNOLOGIES CO., LTD.

CTC Union Technologies Co., Ltd.
Far Eastern Vienna Technology Center
(Neihu Technology Park)
8F, No. 60 Zhouzi St., Neihu, Taipei 114,
Taiwan

T +886-2-26591021
F +886-2-26590237
E sales@ctcu.com
info@ctcu.com
techsupport@ctcu.com
H www.ctcu.com

FRM220-1000EAS Operation Manual

OAM/IP Gigabit Ethernet Media Converter/Switch

~~Version 1.0 September 2008~~
~~Version 2.0 March 2009~~
~~Version 3.0 April 2010~~
~~Version 3.2 May 2010~~
Version 3.21 June 2010

This Manual supports the following models:

FRM220-1000EAS : 2x1000Base-X (SFP) + 2x10/100/1000Base-T
FRM220-1000EAS-1 : 1x1000Base-X (SFP) + 1x10/100/1000Base-T
FRM220-1000EAS-2F : 2x1000Base-X (SFP)
FRM220-1000EA-1 : 1x1000Base-X + 1x10/100/1000Base-T
FRM220-1000EA-2F : 2x1000Base-X

2008-2010 CTC Union Technologies Co., LTD.
All trademarks are the property of their respective owners.
Technical information in this document is subject to change without notice.

ISO 9001 Quality System Certified

Legal
The information in this publication has been carefully checked and is believed to be entirely accurate at the time of publication. CTC Union Technologies assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. CTC Union Technologies reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time and without notice and is not required to update this documentation to reflect such changes.

CTC Union Technologies makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does CTC Union assume any liability arising out of the application or use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

CTC Union products are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use a CTC Union product for any such unintended or unauthorized application, the Buyer shall indemnify and hold CTC Union Technologies and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that CTC Union Technologies was negligent regarding the design or manufacture of said product.

TRADEMARKS
Microsoft is a registered trademark of Microsoft Corp.
HyperTerminal™ is a registered trademark of Hilgraeve Inc.

WARNING:
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause harmful interference in which case the user will be required to correct the interference at his own expense. NOTICE: (1) The changes or modifications not expressively approved by the party responsible for compliance could void the user's authority to operate the equipment. (2) Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

CISPR PUB.22 Class A COMPLIANCE:
This device complies with EMC directive of the European Community and meets or exceeds the following technical standard. EN 55022 - Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment. This device complies with CISPR Class A.

CE NOTICE
Marking by the symbol CE indicates compliance of this equipment to the EMC and LVD directives of the European Community. Such marking is indicative that this equipment meets or exceeds the following technical standards: EN 55022:2006, Class A, EN55024:1998+A1:2001+A2:2003, and EN60950-1:2001

Table of Contents

Chapter 1 Introduction 7
1.1 Welcome 7
1.2 Product Description 7
1.3 Features 7
1.4 Specifications 8
1.5 Management Features 8
1.6 Panel 9
1.7 Factory Reset Procedure 9
Chapter 2 Installation 10
2.1 Chassis Options 10
2.2 Electrical Installation 11
2.3 Installation of SFP Modules 11
2.3.1 Inserting a Bale Clasp SFP Module into the Cage 11
2.3.2 Removing a Bale Clasp SFP Module 11
Chapter 3 Provisioning via Telnet 12
3.1 Introduction 12
3.2 Telnet Login 12
3.2.1 Main Menu 12
3.3 System Configuration 13
3.3.1 Firmware Upgrade 14
3.3.2 Alarm Settings 19
3.3.3 Date & Time Setup 21
3.3.5 Password Setup 21
3.3.5 System Reboot 22
3.3.6 Fiber Port Provisioning 23
3.3.7 Fiber Port 1 Rate Limiting 25
3.3.8 SFP and D/D Functions 25
3.3.9 UTP Port Provisioning 26
3.4 Device Status and Configuration 29
3.5 Advanced Functions 31
3.5.1 Port 1 and Port 2 Trunk Bandwidth 2G 32
3.5.2 Port 1 to Port 2 Mirror 32
3.5.3 Port VLAN (1/3; 2/4) 32
3.5.4 Port 1 and Port 2 Redundancy 32
3.5.5 Static 802.1Q VLAN 33
3.5.6 Static 802.1Q VLAN & Port 1/2 Redundancy 39
3.5.7 802.1Q VLAN Trunk 39
3.5.8 Spanning Tree Protocol 41
3.5.9 Class of Service 45
3.6 OAM Configuration 47
3.6.1 OAM PDU frame size 47
3.6.2 OAM Mode 48
3.7 Link Loss Forwarding 48
3.8 SNMP Configuration 50
3.8.1 General 50
3.8.2 SNMP Operations 50
3.8.3 The Management Information Base 50
3.8.4 MIB Structure 51
3.8.5 SNMP Communities 51
3.8.6 Configuring the SNMP Agent 52
3.8.7 Configuring SNMP Traps 53

Chapter 4 Provisioning Via Web Based Management 54
4.1 Introduction 54
4.2 Web Main Page 54
4.3 System 55
4.3.1 Setup 55
4.3.2 Date & Time 55
4.3.3 Alarm Setting 56
4.4 SNMP 56
4.4.1 Manager 56
4.4.2 Trap 57
4.4.3 System Log 57
4.5 Local Unit Configuration 58
4.5.1 Fiber 1 58
4.5.2 UTP 3 59
4.5.3 Device Status and Configuration 59
4.5.4 Spanning Tree Protocol 60
4.5.5 Static 802.1Q VLAN 60
4.5.6 Counters 63
4.5.7 SFP 64
4.6 Remote Configuration 64

Chapter 1 Introduction

1.1 Welcome

Thank you for choosing the **FRM220-1000EAS** OAM/IP Gigabit Ethernet Media Converter/Switch. Through out this document, all different models of this family will be referred to as **FRM220-1000EAS** or in an abbreviated form as just **1000EAS**. If you would like to skip right to the installation of the converter, proceed to Chapter 2.

This manual is used to explain the hardware installation procedures and operation of the **FRM220-1000EAS**, and present its capabilities and specifications. This manual is divided into 4 chapters, the Introduction, Installation, Telnet Provisioning chapter and Web based provisioning chapter.

Installers should carefully read the Chapter 1&2, Introduction and Installation. The companion document, the **FRM220 NMC Configuration Manual**, is also available in electronic format. The divisions in that manual are intended for use by personnel to answer questions in general areas. Planners and potential purchasers may read the Introduction to determine the suitability of the product to its intended use; Operating Personnel would use the Operations and Web Based Management Chapters and Appendices to become familiar with the line cards and settings. Network Administrators should read the chapters on Operation, Web Based Management and Trouble Shooting to become familiar with the diagnostic capabilities, network settings and management strategies for the SNMP managed chassis.

1.2 Product Description

The **FRM220-1000EAS** is a four port OSI Layer 2 switch and media converter with two Gigabit Ethernet fiber ports (1000Base-X) plus two copper Ethernet ports (10/100/1000Base-T). The Layer 2 switch technologies include tag based VLAN, port trunking, fiber redundancy, 802.1D Spanning Tree Protocol, 802.3x Flow Control and ingress/egress bandwidth control per port. With its own embedded 32 bit processor, the **1000EAS** supports stand-alone management via IP (Telnet, SNMP & HTTP) or in-band management via 802.3ah-OAM protocol when connected to another **1000EAS** in point to point or as a CPE device to a **1000EAS** mounted in the **FRM220** managed media converter rack.

1.3 Features

- Four port L2 switch
- Port based VLAN support (1000EAS model)
- Tag VLAN support
- Double VLAN tag support (Q-in-Q)
- Cisco Trunk Management VID support
- Ingress/Egress Bandwidth control
- Spanning Tree Protocol support
- 32bit embedded CPU for stand-alone management
- 802.3ah-OAM in-band management
- Firmware upgrade via TFTP
- Telnet, HTTP, SNMP and OAM management
- Dying gasp (remote power failure detection)
- Auto Laser Shutdown
- Link Fault Pass-Through (LFP)
- Fiber Redundancy function
- Paused Frame flow-control
- Digital Diagnostic (DOM) SFP support
- RMON counters
- SNTP client

WARNING: Fiber optic equipment may emit laser or infrared light that can injure your eyes. Never look into an optical fiber or connector port. Always assume that fiber optic cables are connected to a laser light source.

1.4 Specifications

- **Optical Interface**
- **Connector** SFP cage (depending on model)
- **Data rate** 1.25Gb/s
- **Duplex mode** Full duplex
- **Fiber** MM 50/125um, 62.5/125um
  SM 9/125um (depending on SFP)
- **Distance** MM 550M/2KM,
  SM 15/30/50/80/120KM (depending on SFP)
- **Wavelength** Depends on SFP and model
- **Electrical Interface**
- **Connector** RJ-45
- **Data Rates** 10Mbps, 100Mbps, 1000Mbps
- **Duplex** Full or Half Duplex
- **Cable** 10Base-T Cat. 3,4,5,5e UTP
- 100Base-TX Cat. 5, 5e or higher
- 1000Base-T Cat 5, 5e, 6 or higher
- **Standards** IEEE802.3, 802.3u, 802.3z, 802.3ab, 802.3ah
  802.3x, 802.1D, 802.1p, 802.1Q, RFC 4330 (SNTP)
- **Maximum MTU** 1632 bytes
- **Indications** LED (PWR, Fiber 1&2 Link, Test, UTP 3&4 Link, UTP 3&4 Speed)
- **Power** (Card supports hot-swapping)
- **Input** Card : 12VDC, Standalone : AC, DC options
- **Consumption** <8W
- **Dimensions** 155 x 88 x 23mm (D x W x H)
- **Weight** 120g
- **Temperature** 0 ~ 50°C (Operating), -10 ~ 70°C (Storage)
- **Humidity** 10 ~ 90% non-condensing
- **Certification** CE, FCC, LVD, RoHS
- **MTBF** 65000 hrs (25°C)

1.5 Management Features

The **FRM220-1000EAS** has its own embedded processor which can be used to configure the device for stand-alone operation. When placed in a stand-alone chassis, this device supports a text based Telnet terminal with an easy to use menu system for configuration. The embedded **HTTP** server provides an easy to use **GU**I (Graphical User Interface) with any web browser. **SNMP** is also supported in the stand-alone operation. When using network management software and our proprietary MIB file specifically for the **1000EAS,** all settings can be performed, performance monitoring realized and alarm traps received. When placed in a managed chassis, such as our **FRM220-CH20** with **NMC** (Network Management Controller) card, the **1000EAS** card is configured and monitored through the chassis **NMC** via console, Telnet, Web HTTP or SNMP.

1. Stand-alone – IP settings allow management by Telnet, Web or SNMP
2. Rack management - When placed in **NMC** managed rack, all other settings can be overridden by the **NMC** management.

1.6 Panel

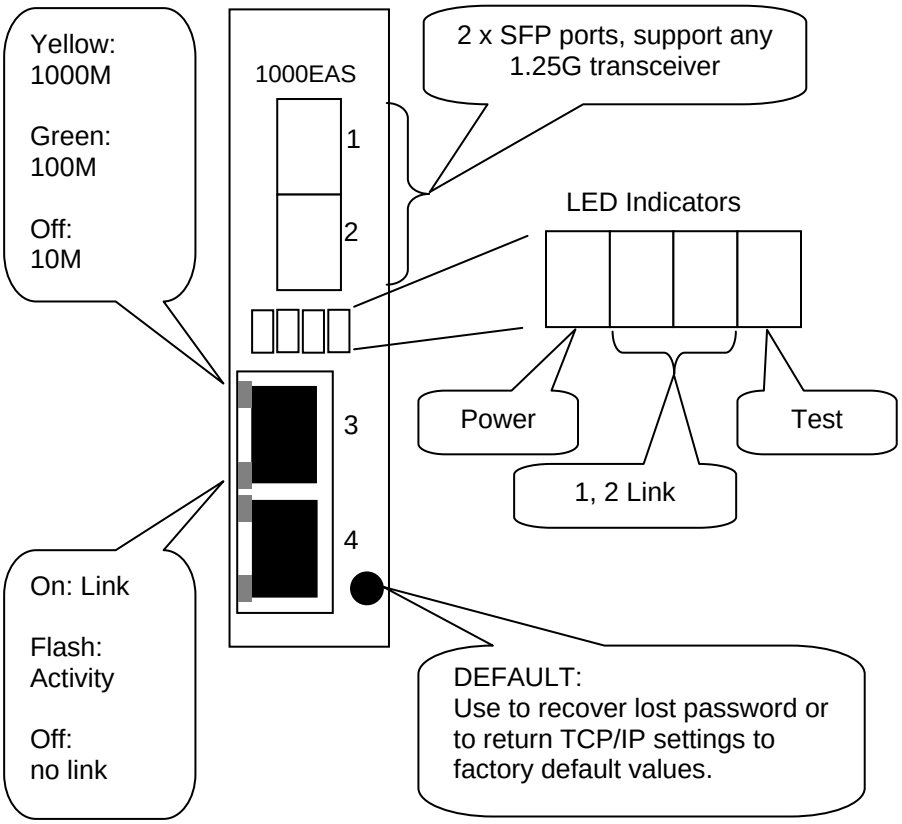


Figure 1.1 Panel designations of **FRM220-1000EAS**

1.7 Factory Reset Procedure

Apply power to the **1000EAS** and allow 30 seconds to fully boot. Using a pencil or ball-point pen, press the 'DEFAULT' recessed push-button switch (located on the face plate) and hold for 9~10 seconds. DO NOT POWER OFF. Allow the unit to again fully reboot. The defaults are:

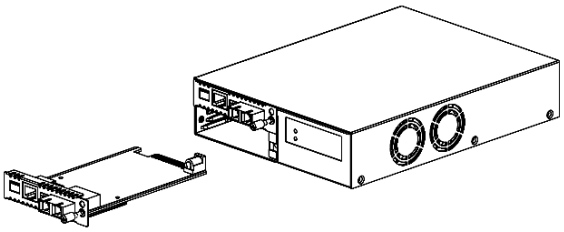
IP=10.1.1.1
netmask=255.0.0.0
GW=10.1.1.254
TFTP server=10.1.1.100

The username and password are both reset to 'admin' if enabled.

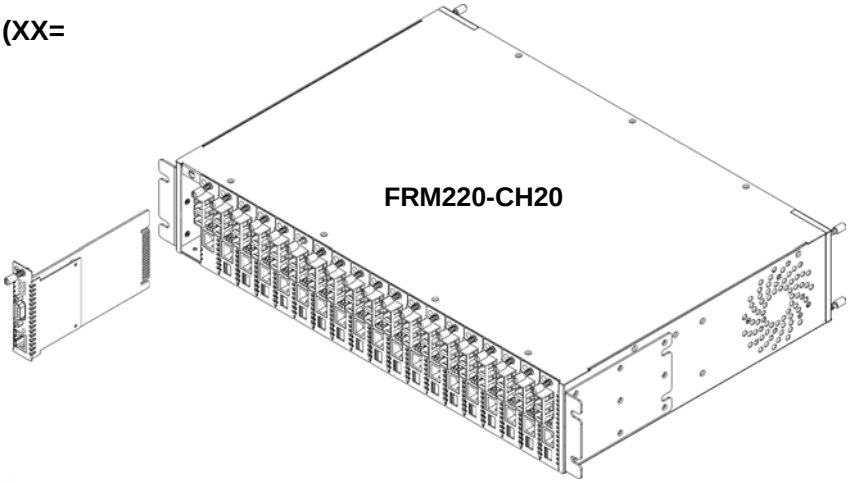
Chapter 2 Installation

2.1 Chassis Options

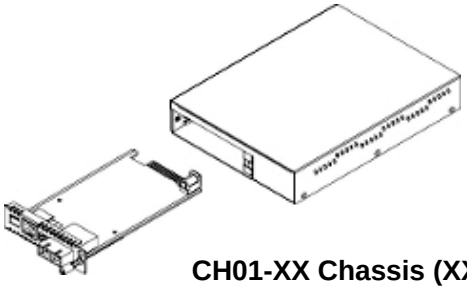
Note: This converter card can be placed in any **FRM220** series chassis, including the single slot CH-01, two slot CH02-NMC or the full twenty slot CH-20 chassis. Chassis with built-in power are available with single AC (90-240VAC), single DC (18~75VDC), dual AC, dual DC or AC plus DC combo. The single slot chassis with external power adapter works with AC source voltage only with the provided 90~240VAC 12VDC@400mA switching adapter.



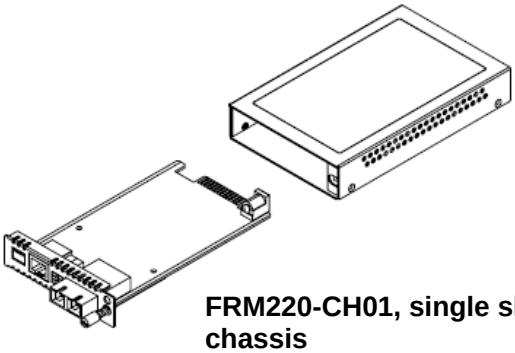
CH02-NMC-XX Chassis (XX= AC, DC, AA, DD or AD)



FRM220-CH20



CH01-XX Chassis (XX= AC, DC, AA, DD or AD)



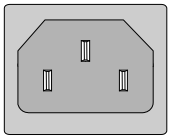
FRM220-CH01, single slot chassis
Requires external AC to DC 12V switching adapter.

Figure 2.1 Chassis options for **FRM220-1000EAS** card

Follow all ESD precautions when handling the card and SFP modules.

2.2 Electrical Installation

With a built-in AC power chassis, AC power is supplied to the chassis through a standard IEC C14 3-prong receptacle, located on the rear of the chassis. Any national power cord with IEC C13 line plug may be used to connect AC power to the power module. With a built-in DC power chassis, DC -48V is connected to the terminal block located on the rear of the chassis, observing the proper polarity. The chassis should always be grounded through the protective earth lead of the power cable in AC installations, or via the frame ground connection for DC installations.



Left: Live line
Right: Neutral line
Middle: Ground

IEC C13 line plug

DC IN
-V FG +V

Left: -V (-48V)
Right: +V (0V)
Middle: Frame Ground

18~75 VDC

Figure 2.2 IEC (AC) & terminal block (DC) power connector pin assignment

2.3 Installation of SFP Modules

CTC Union supplied SFP modules are of the Bale Clasp type. The bale clasp pluggable module has a bale clasp that secures the module into the SFP cage.

2.3.1 Inserting a Bale Clasp SFP Module into the Cage

Step 1 Close the bale clasp upward before inserting the pluggable module.
Step 2 Line up the SFP module with the port, and slide it into the cage.

2.3.2 Removing a Bale Clasp SFP Module

Step 1 Open the bale clasp on the SFP module. Press the clasp downward with your index finger.
Step 2 Grasp the SFP module between your thumb and index finger and carefully remove it from the SFP cage.

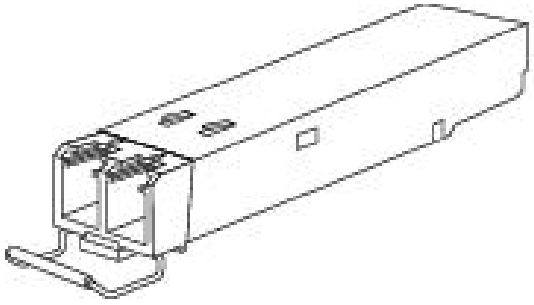


Figure 2.3 Bale Clasp type SFP with bale open

Chapter 3 Provisioning via Telnet

3.1 Introduction

The **FRM220-1000EAS** is accessible through a TCP/IP network over Ethernet. The Telnet protocol is employed to provide an easy to use, text based, menu system for performing all configuration functions. In most cases, we recommend that the networking engineer start configuration by using Telnet. Configure the required TCP/IP parameters for the network deployment, and then continue detailed configurations using the web based GUI. For GUI operation, please refer to chapter 4.

3.2 Telnet Login

Connect one of the copper Ethernet ports to a PC. Configure the PC to the same subnet as the **FRM220-1000EAS** (recommend 10.1.1.100). Use Telnet protocol (port 23) to connect to the **1000EAS**. If the password has been enabled, then the factory default will be 'admin/admin'.

3.2.1 Main Menu

The Telnet operation of the **1000EAS** uses a simple menu system. From the main menu, using ESC will prompt for a logout. It is recommended to use the logout function after finishing configuration or monitoring of the **1000EAS** so that the Telnet session connection is closed normally. The menu items are selected by simply keying in the menu item's number (in the < > brackets). Some parameter settings are toggled by a single key stroke, while others are selected from additional sub-menus. Unless advised that the unit requires a reboot, all settings take effect immediately.

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ********************************************
Fiber 1   [Link Up       ] [Remote LB: Off  ]
Fiber 2   [Link Up       ] [Remote LB: Off  ]
UTP   3   [Link Up       ] [Speed: 1000M] [Duplex: Full]
UTP   4   [Link Up       ] [Speed:  100M] [Duplex: Full]
Remote A Module    [1000EAS     ]
Remote B Module    [1000EAS     ]
Port 1 OAM Mode    [Active ]
Port 2 OAM Mode    [Active ]
Advance Functions  [Normal ]

 <L> :Local    Status and Configuration.
 <A> :Remote A Status and Configuration.
 <B> :Remote B Status and Configuration.
 <M> :SNMP Manager.
 <S> :System Configuration.

<ESC>:Logout.
```

Figure 3.1 Main menu

3.3 System Configuration

Select item 'S' from main menu, ***System Configuration***

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< System Configuration >>
Version                  [1.200-3.240-0.000-0.000]
MAC Address              [00:02:AB:FF:FE:02]
NMC Action               [Inactive (Stand alone)]

 <1> :IP Address         [59.125.162.248]
 <2> :Subnet Netmask     [255.255.255.240]
 <3> :Default Gateway IP [59.125.162.241]
 <4> :Host Name          [1000eas]
 <5> :TFTP Server IP     [59.125.162.243]
 <6> :TFTP File Name     [bootpImage]
 <7> :Do TFTP and Update Firmware.
 <A> :Alarm Settings.
 <T> :Date and Time.
 <L> :Password Setting.
 <R> :System Rebooting.

<ESC>:Go to Previous Menu.
```

Figure 2.5 System Configuration menu

<1> **IP Address** : This is the IPv4 32 bit Internet Protocol decimal formatted address used to identify this device over the network.
<2> **Subnet Mask** : The process of subnetting is the division of a computer network into groups of computers that have a common, designated IP address routing prefix.
<3> **Default Gateway IP** : A default gateway is the node on the computer network that is chosen when the IP address does not match any other routes in the routing table.
<4> : **Host Name** : A hostname is a label that is assigned to a device connected to a computer network and that is used to identify the device in various forms of electronic communication such as on the World Wide Web.
<5> **TFTP Server IP** : Trivial File Transfer Protocol (TFTP) is a file transfer protocol, with the functionality of a very basic form of File Transfer Protocol (FTP). This setting is the IP address of the TFTP server.
<6> **TFTP File Name** : This is the filename (case sensitive) of the firmware image that is placed on the TFTP server and that must be downloaded by the TFTP client in the **FRM220-1000EAS**.
<7> **Do TFTP and Update Firmware** : This command will start the upgrade process. First the image file will be downloaded into local RAM. If the image is not found or transfer fails, the upgrade process will abort. Once the image is successfully downloaded, it is check to be sure it is the proper image for the right model. At this point, if all is successful, the Flash will be erased and then reprogrammed with the new image. Any power failure during the erase and re-write will result in a 'bricked' unit. There is no recovery except to return to factory where the flash chip must be manually replaced. **DO NOT ALLOW ANY POWER INTERRUPTION DURING FLASHING**.
<A> **Alarm Settings** : This item will bring up a sub-menu for alarm settings. Alarms are indications of fiber or UTP link failure as well as remote converter power failure (dying gasp). Alarms are grouped into two categories; Major Alarms or Minor Alarms. When any alarm occurs, it is then sent as an unsolicited SNMP trap message. For more detailed information please see section 3.3.2.
<T> **Date and Time** : This item will bring up a sub-menu for the Simple Network Time Protocol (SNTP) settings. For more detailed information please see section 3.3.3.
<L> **Password Setting** : This item will bring up a sub-menu for password authentication settings. For more detailed information, please refer to section 3.3.4.
<R> **System Rebooting** : This menu item is used to do a "warm boot" of the **1000EAS**. Any changes to the TCP/IP settings will become active after rebooting.
<ESC> : Pressing the escape key will leave the configuration menu and go back to the main menu.

3.3.1 Firmware Upgrade

Occasionally, **CTC Union** will release new firmware for their products. If new functions are added through software modification or if programming errors are uncovered and resolved, those items will be listed in the firmware ***release note*** which is included in an 'upgrade package' along with a detailed upgrade procedure and the firmware image code.

The ***System Configuration*** menu is where new firmware may be applied to the **1000EAS**. The firmware is uploaded to the agent using Trivial File Transfer Protocol. Once the TFTP server's IP is configured and the image file name matches the update image placed in the TFTP root or path, item #7 will start the upload process. Once the image has been uploaded into memory (approximately 20 seconds), and the check-sum and image ID confirmed, the flash memory will be erased and the image written to the flash memory (non-volatile memory). Following successful flash writing (approximately 50 seconds), the **1000EAS** will automatically reboot.

WARNING: Never allow any power disruption during the flash erasing and writing process.

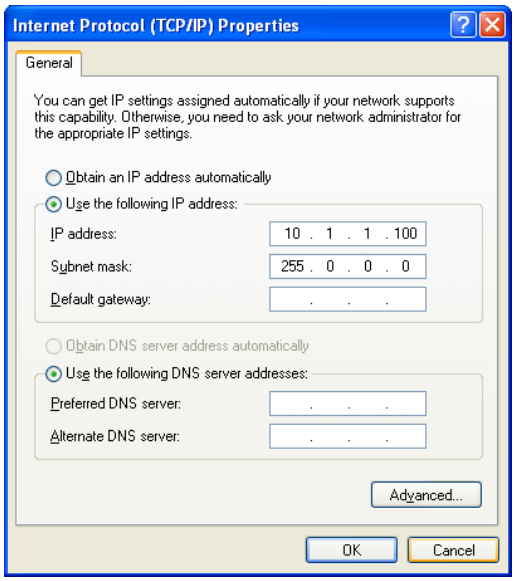
Prerequisites:
1. **FRM220-1000EAS** in **FRM220-CH20** Chassis with **NMC** or in **FRM220-CH1** stand-alone single slot.
(Includes models **1000EAS**, **1000EAS-1**, **1000EA-1**, **1000EAS-2F**, and **1000EA-2F**.)
2. **FRM220-1000EAS must be version 2.009 or above to upgrade to latest 3.X.** (if not please do upgrade to v2.009 first)
3. Cat 5e or above Ethernet patch cable
4. Laptop or PC, TCP/IP ready
5. Telnet client software (PuTTY or HyperTerminal)
6. TFTP server (or **CTCU TFTP Server** for Windows)
7. Upgrade firmware, for version 3.xxxx, released as 'bootpImage' image files for each model.

Procedure:
Step 1. Connect the **1000EAS** Ethernet to the desktop's or laptop's Ethernet port with 1:1 UTP patch cable. (**2F** models require another media converter to connect electrical to fiber.)

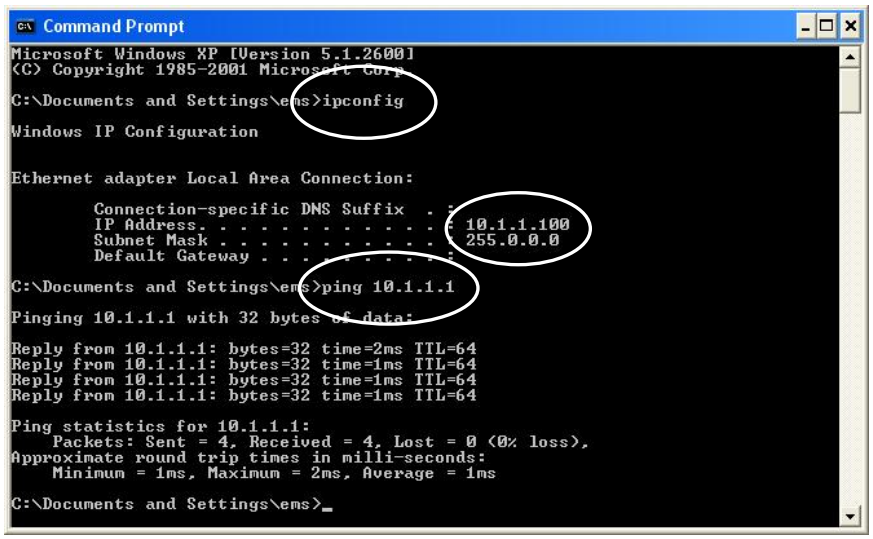
Step 2. If the IP address in unknown, power on **1000EAS** and wait until fully booted (minimum 20 seconds). With pen or pencil point, press and hold the 'DEFAULT' switch, located on the lower-right face of converter, for 6-10 seconds. Allow to fully boot again (about 30 seconds). This will restore the converter to factory default and known parameters.

Step 3. Configure TCP/IP settings on the desktop or Laptop's Ethernet LAN port for:

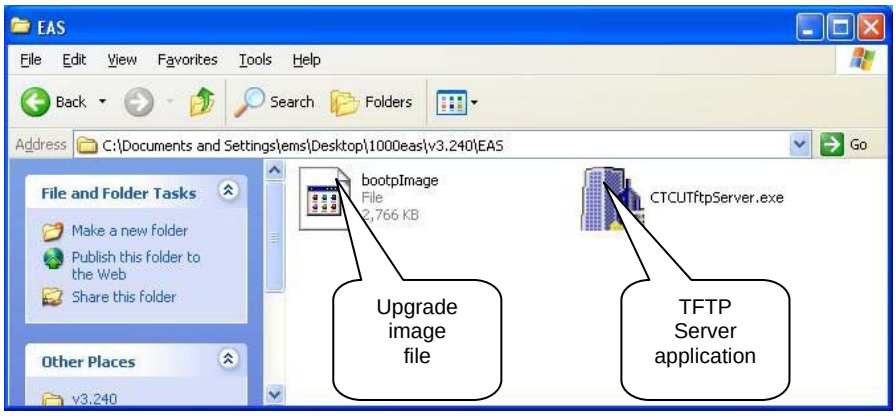
a. static IP 10.1.1.100
b. subnet mask 255.0.0.0
c. gateway not necessary

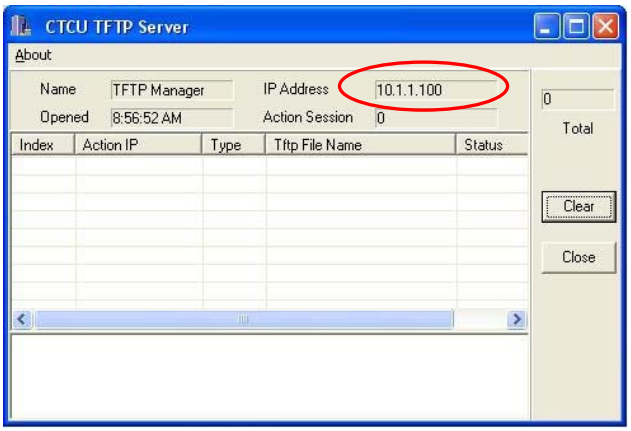

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
10 . 1 . 1 . 100
Subnet mask:
255 . 0 . 0 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Step 4. Open a command window on the laptop or desktop PC (for example click 'Start' button, click 'Run' and enter 'cmd' in the Run window and click 'OK'). Check the TCP/IP settings with the 'ipconfig' command and then 'ping' the **FRM220-1000EAS**. Make sure the network connection works and is reliable. (note: if ping times out, try doing 'arp –d' command, then if still unsuccessful check cables.)

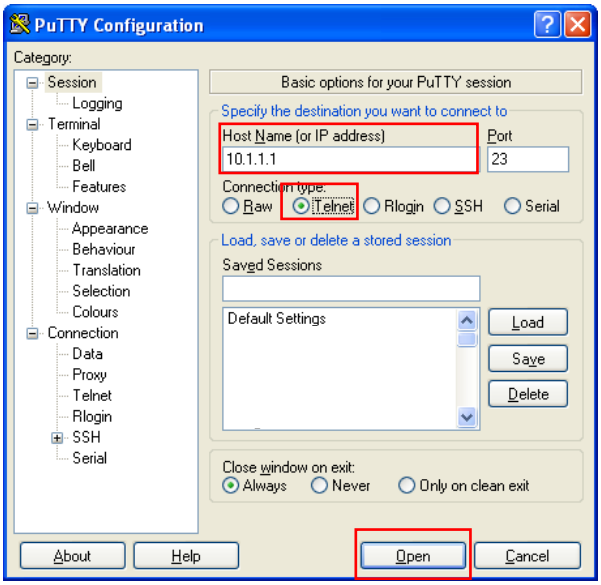

Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\ems>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 10.1.1.100
Subnet Mask . . . . . : 255.0.0.0
Default Gateway . . . . . :
C:\Documents and Settings\ems>ping 10.1.1.1
Pinging 10.1.1.1 with 32 bytes of data:
Reply from 10.1.1.1: bytes=32 time=2ms TTL=64
Reply from 10.1.1.1: bytes=32 time=1ms TTL=64
Reply from 10.1.1.1: bytes=32 time=1ms TTL=64
Reply from 10.1.1.1: bytes=32 time=1ms TTL=64
Ping statistics for 10.1.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Documents and Settings\ems>_

Step 5. Start the TFTP application program by double-clicking. It was extracted with the upgrade package. If the firewall complains, select 'Unblock'. Make sure the 'bootpImage' file is located in the same directory as the TFTP application program. The IP Address shown in the TFTP server application should be the IP of your PC (10.1.1.100 in this case).





Step 6. Start the Telnet client program of your choice. In this example we are using the PuTTY program, which is open source, free, and very popular with network engineers.



Key-in the IP address, select the 'Telnet' radio button and then click 'Open'.

Step 7. The upgrade is performed by first selecting 'S', "**System Configuration**" menu.

The following screens are examples of main menu of **FRM220-1000EAS**, version 3.000.

Warning: The version must be at least 2.009. If not, **STOP**, download the update to version 2.009 first, perform upgrade, then proceed with upgrade to any version 3.xxx. If your unit is not at version 2.009, the TFTP download will timeout and the upgrade will abort.

Step 8. Make sure the settings are correct. The screens below are what they should be if the FRM220-1000EAS has been returned to its factory default setting. Confirm that the TFTP server IP matches your PC or Laptop and that the image filename matches our upgrade file name. Press the '7' key "TFTP Download File System".

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.000      ***
          ********************************************
<< System Configuration >>
Version                    [1.200-3.000-0.000-0.000]
MAC Address                [00:02:AB:FF:FE:02]
NMC Action                 [Inactive (Stand alone)]

 <1> :IP Address           [10.1.1.1]
 <2> :Subnet Netmask       [255.0.0.0]
 <3> :Default Gateway IP   [10.1.1.254]
 <4> :Host Name            [1000eas]
 <5> :TFTP Server IP       [10.1.1.100]
 <6> :TFTP File Name       [bootpImage]
 <7> :Do TFTP and Update Firmware.
 <A> :Alarm Settings.
 <T> :Date and Time.
 <L> :Password Setting.
 <R> :System Rebooting.

<ESC>:Go to Previous Menu.
```

You will be prompted for a final Yes or No.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.000     ***
          ******************************************
<< System Configuration >>
Version                   [1.200-3.000-0.000-0.000]
MAC Address               [00:02:AB:FF:FE:02]
NMC Action                [Inactive (Stand alone)]

 <1> :IP Address          [10.1.1.1]
 <2> :Subnet Netmask      [255.0.0.0]
 <3> :Default Gateway IP  [10.1.1.254]
 <4> :Host Name           [1000eas]
 <5> :TFTP Server IP      [10.1.1.100]
 <6> :TFTP File Name      [bootpImage]
 <7> :Do TFTP and Update Firmware.
 <A> :Alarm Settings.
 <T> :Date and Time.
 <L> :Password Setting.
 <R> :System Rebooting.
================================
Download F/W  (Y/N)
```

Step 9. Press the 'Y' key to start TFTP transfer and update. The message like "Write bootpImage to memory" will be displayed. The file transfer takes about 20 seconds.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.000     ***
          ******************************************
<< System Configuration >>
Version                   [1.200-3.000-0.000-0.000]
MAC Address               [00:02:AB:FF:FE:02]
NMC Action                [Inactive (Stand alone)]

 <1> :IP Address          [10.1.1.1]
 <2> :Subnet Netmask      [255.0.0.0]
 <3> :Default Gateway IP  [10.1.1.254]
 <4> :Host Name           [1000eas]
 <5> :TFTP Server IP      [10.1.1.100]
 <6> :TFTP File Name      [bootpImage]
 <7> :Do TFTP and Update Firmware.
 <A> :Alarm Settings.
 <T> :Date and Time.
 <L> :Password Setting.
 <R> :System Rebooting.
================================
Download F/W  (Y/N)
Write bootpImage to memory. Please wait.
```

After the file transfer, approximately 50 seconds will be required for the flash to be written, followed by the unit automatically performing a "warm boot". Do not close the Telnet session or allow any power interruption during the upgrade process.

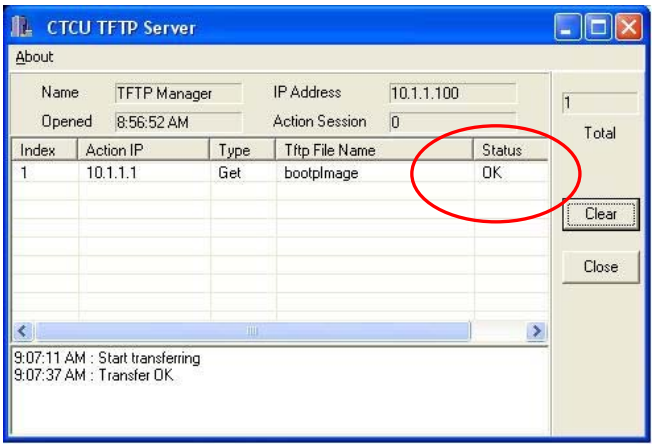
DO NOT CLOSE THE WINDOW OR ALLOW ANY POWER INTERRUPTION!!!! THIS IS VERY IMPORTANT.

The flash writing takes at least 50 seconds. The progress bar gives an approximation of the percent completed. When complete, the "Rebooting …" message will be displayed. **DO NOTHING!!**

```
############################################################
file_size=3101724 bytes
Don`t close the window or power before printing write done
0%                                                    100%
|-------------------------------------------------|
#################################################

Rebooting ...
```

Step 10. After update, the **FRM220-1000EAS** will automatically reboot. The current Telnet session will close. (During reboot, all LEDs will first go out, then all LEDs will light. The "Test" LED will extinguish first and a few seconds later the LEDs will return to normal running and link states.)

Check that the TFTP transfer was normal with the 'OK' status.



Step 11. Use Telnet client and login to the **FRM220-1000EAS** again.

The following screen shows the **1000EAS** updated to 3.240. For a newer version, these numbers should reflect the new version.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< System Configuration >>
Version                   [1.200-3.240-0.000-0.000]
MAC Address               [00:02:AB:FE:FE:02]
NMC Action                [Inactive (Stand alone)]

 <1> :IP Address          [10.1.1.1]
 <2> :Subnet Netmask      [255.0.0.0]
 <3> :Default Gateway IP  [10.1.1.254]
 <4> :Host Name           [1000eas]
 <5> :TFTP Server IP      [10.1.1.100]
 <6> :TFTP File Name      [bootpImage]
 <7> :Do TFTP and Update Firmware.
 <A> :Alarm Settings.
 <T> :Date and Time.
 <L> :Password Setting.
 <R> :System Rebooting.

<ESC>:Go to Previous Menu.
```

Continue with normal TCP/IP re-configuration and provisioning.

3.3.2 Alarm Settings

From the **Alarm Settings** menu, we can configure and assign different alarm conditions to either major or minor alarm status. In this way, the network administrator can determine which alarm conditions should be responded to with the highest priority, or which alarms do not need high priority responses.

From the Main Menu, select the <S> (System Configuration) and from this menu select <A> (Alarm Settings).

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Alarm Settings >>
Major Alarm Status [Inactive]
Minor Alarm Status [Inactive]

 <1> :Major Alarm    [Disable]
 <2> :Minor Alarm    [Disable]
 <3> :Major Local  Alarm Settings.
 <4> :Major Remote Alarm Settings.
 <5> :Minor Local  Alarm Settings.
 <6> :Minor Remote Alarm Settings.

<ESC>:Go to Previous Menu.
```

In the following example, the local Major alarm indication is presented whenever any of the "checked" events occur. Fiber link down or remote power failure will be reported as Major alarms.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Major Local Alarm Settings >>
 <1> :[*]Fiber 1 Link Down
 <2> :[*]Fiber 2 Link Down
 <3> :[ ]UTP   3 Link Down
 <4> :[ ]UTP   4 Link Down
 <5> :[*]Remote A Power OFF
 <6> :[*]Remote B Power OFF

<ESC>:Go to Previous Menu.
```

Like wise, Minor alarms can also be assigned by events. This example shows the local Minor alarms are reported only if UTP links are down.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Minor Local Alarm Settings >>
 <1> :[ ]Fiber 1 Link Down
 <2> :[ ]Fiber 2 Link Down
 <3> :[*]UTP   3 Link Down
 <4> :[*]UTP   4 Link Down
 <5> :[ ]Remote A Power OFF
 <6> :[ ]Remote B Power OFF

<ESC>:Go to Previous Menu.
```

In setting of the local and remote units, Major and Minor alarms are key when network management via SNMP is used. When enabled here and when SNMP trap receivers are configured, Major and Minor alarm conditions will be reported through the SNMP trap mechanism.

3.3.3 Date & Time Setup

The date and time setup are important so that any trap messages generated by the SNMP agent will have the correct timestamp. The **1000EAS** supports setting time manually or automatic time configuration through the use of **NTP** (Network Time Protocol) or **SNTP** (Simple Network Time Protocol).

From the Main Menu, select the <S> (System Configuration) and from this menu select <T> (Date and Time).

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Date and Time >>
Current Date And Time [2010-04-14/06:09:23 Fri]
Time Server IP        [220.130.158.71]
Time Zone             [GMT +00:00]
Auto Adjust Time      [Disable]

 <1> :Adjust Current Time.
 <2> :Set Time Server IP.
 <3> :Set Time Zone.
 <4> :Enable/Disable Auto Synchronize Time.
 <5> :Synchronize Time with NTP Server.

<ESC>:Go to Previous Menu.
```

1. **Adjust Current Time** – Use this menu item to manually adjust the date and time.
2. **Set Time Server IP** – The time server IP is the IP address of a NTP server that provides time synchronization services on a network. Geographically close servers should be chosen from the pool of NTP servers.
3. **Set Time Zone** – All network time is synchronized to UTC (Coordinated Universal Time) which is based on International Atomic Time. The time zone setting will let the UTC time appear correctly for your geographic location. Time zone settings are + (East) or – (West) full or half hours from UTC coordinates or previously known as GMT (Greenwich Mean Time).
4. **Enable/Disable Auto Synchronize Time** – When auto synchronization is enabled, the SNTP daemon in the **1000EAS** will poll and update time from the time server once every hour.
5. **Synchronize Time with NTP Server** – This action will cause the SNTP daemon to immediately poll and update date and time with the NTP server. The results will either be a 'timeout' or the time will be successfully synchronized.

3.3.5 Password Setup

Access to the **1000EAS** via Telnet or Web is controlled by the use of user passwords. One user ID account can be created and assigned password for authentication. The management interface can only then be accessed by using the correct username and password.

From the Main Menu, select the <S> (System Configuration) and from this menu select <L> (Password Setting).

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Password Configuration >>
 <1> :Login Password      [Disable]
 <2> :Set New UID and Password.

<ESC>:Go to Previous Menu.
```

1. **Login Password** – Enable or disable the password authorization feature.
2. **Set New UID and Password** – Key-in username and password for management authentication. If the password is lost, the unit must be reset to factory default. See section 1.7.

3.3.5 System Reboot

The system reboot feature allows an operator to remotely cause the 1000EAS to do a 'warm boot'. The system reboot will send a reset signal to both the embedded CPU chip and to the L2 switch chip. The CPU will then reboot the kernel and reinitialize the switch chip with the stored configuration settings.

Caution should be exercised when doing a system reset as all traffic through all ports of the device will be blocked until the switch chip is initialized. In addition, the OAM discovery and negotiation will need to redo. If enabled, STP (Spanning Tree Protocol) discovery will need to rebuild path tables.

From the Main Menu, select the <S> (System Configuration) and from this menu select <R> (System Rebooting). Confirmation is required.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.240      ***
          ******************************************
<< System Configuration >>
Version                   [1.200-3.240-0.000-0.000]
MAC Address               [00:02:AB:FF:FE:02]
NMC Action                [Inactive (Stand alone)]

 <1> :IP Address          [59.125.162.248]
 <2> :Subnet Netmask      [255.255.255.240]
 <3> :Default Gateway IP  [59.125.162.241]
 <4> :Host Name           [1000eas]
 <5> :TFTP Server IP      [59.125.162.243]
 <6> :TFTP File Name      [bootpImage]
 <7> :Do TFTP and Update Firmware.
 <A> :Alarm Settings.
 <T> :Date and Time.
 <R> :System Rebooting.
-------------------------------------------------------------
 Reboot System ?

 <0><N> No          <1><Y> Yes
```

When the **1000EAS** warm starts the process is almost identical to a cold start.

1. The switch chip is reset at which point all traffic is blocked.
2. The CPU is reset.
3. The boot process is started from the bootloader read from flash.
4. The bootloader instructs the CPU to copy the image from flash and decompress into RAM.
5. Once the image has decompressed into ram, the CPU continues to execute program from RAM.
6. The previous network settings stored in serial EPROM are used to configure the device's network configuration.
7. The configuration settings stored in the serial EPROM are read and the settings are programmed into the switch chip.
8. Traffic will then start to transmit through the switch normally.
9. If OAM is enabled, the OAM discovery will occur.
10. If STP is enabled, the switch won't start to forward packets until the path tables are rebuilt through learning.

3.3.6 Fiber Port Provisioning

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.240      ***
          ********************************************
Fiber 1   [Link Up       ] [Remote LB: Off  ]
Fiber 2   [Link Up       ] [Remote LB: Off  ]
UTP   3   [Link Up       ] [Speed:  100M] [Duplex: Full]
UTP   4   [Link Down     ] [Speed: -----] [Duplex: ----]
Remote A Module    [1000EAS     ]
Remote B Module    [1000EAS     ]
Port 1 OAM Mode    [Active ]
Port 2 OAM Mode    [Active ]
Advance Functions  [Normal ]

 <L> :Local    Status and Configuration.
 <A> :Remote A Status and Configuration.
 <B> :Remote B Status and Configuration.
 <M> :SNMP Manager.
 <S> :System Configuration.
```

Select item 'L' from the main menu.

From the ***Local Status and Configuration*** menu, each port can be managed (activated or disabled, speed & duplex set, ingress & egress bandwidth rates set, and diagnostic loop back performed) and monitored (link status, RMON counters, DD functions, dying gasp) individually per port. Select port number. Select items by number/letters.

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.240      ***
          ********************************************
<< Local Status and Configuration >>
NMC Action    [Inactive (Stand alone)]

 <1> :Fiber 1 Status and Configuration.
 <2> :Fiber 2 Status and Configuration.
 <3> :UTP   3 Status and Configuration.
 <4> :UTP   4 Status and Configuration.
 <D> :Device  Status and Configuration.
 <Q> :Static 802.1Q VLAN Status and Configuration.
 <S> :Spanning Tree Status and Configuration.
 <L> :Link Loss Forwarding Configuration.
 <C> :Counters Status and Configuration.

<ESC>:Go to Previous Menu.
```

Select the first fiber port by keying "1" at the console.

3.3.6.1 Fiber Port 1 Provisioning

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.273     ***
          ******************************************
<< Local Fiber 1 Status and Configuration >>
Link Status              [Link Up  ]
Remote Device Power      [OK]
OAM Remote Loopback Test [OFF]
OAM Looped               [OFF]

 <1> :Port Active           [Enable ]
 <2> :Auto Laser Shutdown   [Disable]
 <3> :OAM Channel A Mode    [Active ]
 <4> :Remote Loopback Test  [Disable]
 <5> :Ingress Rate Limit    [Unlimited]
 <6> :Egress  Rate Limit    [Unlimited]
 <7> :Default Port CoS      [0]
 <S> :SFP and D/D Function  [Yes]

<ESC>:Go to Previous Menu.
```

<1> **Port Active** : When disabled, this port will no longer transfer any data and the link will be down.
<2> **Auto Laser Shutdown** : This safety feature, when enabled, will disable the transmit laser if there is no received signal. It is also referred to as 'ALS'.
<3> **OAM Channel A Mode** : The OAM can be disabled or enabled. Within an OAM broadcast link, there should only be one 'active' unit and other unit should be 'passive'.
<4> **Remote Loopback Test** : This function enables or disables the remote OAM loopback test. When active, OAM loopback frames are sent and the remote equipment should acknowledge them. The link integrity can be confirmed without using IP protocol.
<5> & <6> **Ingress/Egress Rate Limit** : These bandwidth control settings are explained in more detail under the section 3.3.7.
<7> **Default Port CoS** : The Class of Service is a 3 bit field within an Ethernet frame header when using 802.1Q tagging. The field specifies a priority value of between 0 and 7 inclusive that can be used by Quality of Service (QoS) disciplines to differentiate traffic. When 802.1Q is not enabled, there is no tag and therefore no 802.1p tag priority. Use this setting to set the default CoS for this port (0 to 7).
<S> **SFP and D/D Function** : The MSA (Multi-Source Agreement) information can be displayed for the inserted SFP module. An example is shown in section 3.3.8.

3.3.7 Fiber Port 1 Rate Limiting

The **1000EAS** provides per port ingress and egress rate limiting. For bandwidth settings, IRL or ingress rate limit refers to limiting any packets coming into the converter, while ERL or egress rate limit refers to limiting packets leaving the converter. When rate limiting is applied, ERL will use pause commands (802.3X) when the desired rate limit is exceeded, while any IRL setting will cause packet to be dropped when the limit is exceeded. This is an important point when doing the rate limit settings. It is preferable to set ERL at each port for the path that requires limiting so that flow control can help connected devices cope with the limiting. If IRL is employed, a connected device which has its packets dropped without flow control, will continue to send packets at its full rate. Also, since the packets are dropped, the application layer can only deal with the packet loss by timing out.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Local Fiber 1 Status and Configuration >>
Link Status               [Link Up  ]
Remote Device Power       [OK]
OAM Remote Loopback Test  [OFF]
OAM Looped                [OFF]
_____________________________________________________________________________
_____________
 Select Ingress Rate Limit.

<0> Unlimited     <1> 250M          <2> 140M          <3> 95M
<4> 57M           <5> 40M           <6> 31M           <7> 25M
<8> 20M           <9> 14M           <A> 10M           <B> 8M
<C> 6M            <D> 4M            <E> 3M            <F> 2M
<G> 1M            <H> 960K          <I> 896K          <J> 832K
<K> 768K          <L> 705K          <M> 640K          <N> 576K
<O> 512K          <P> 448K          <Q> 384K          <R> 320K
<S> 256K          <T> 192K          <U> 128K          <V> 70K

<ESC>:Previous Menu.
```

The ingress rate setting menu. Select rate from 70K to 250M or unlimited.

The same setting rates can be applied to the egress direction.

3.3.8 SFP and D/D Functions

Modern optical SFP transceivers support digital diagnostics monitoring (DDM) functions according to the industry-standard SFF-8472. This optional feature in SFP is also known as digital optical monitoring (DOM) and gives the end user the ability to monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, etc. DDM is not available in every SFP, so if the function says 'No' then the inserted SFP does not support DD. To view this menu, press "S" from the Fiber Status and Configuration menu.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Local Fiber 1 SFP and D/D Function >>
Vendor Name           [FIBERXON INC.   ]
Vendor Part Number    [FTM-3125C-L40   ]
Fiber Type            [Single]
Tx Wave Length        [1310 nm]
Rx Wave Length        [1310 nm]
Link Length           [40 km]
TX Power              [0 dBm]
RX Power              [-12 dBm]
RX Sensitivity        [0 dBm]
Temperature           [54 degree C]

<ESC>:Go to Previous Menu.
```

3.3.9 UTP Port Provisioning

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.240      ***
          ********************************************
Fiber 1   [Link Up       ] [Remote LB: Off  ]
Fiber 2   [Link Up       ] [Remote LB: Off  ]
UTP   3   [Link Up       ] [Speed:  100M] [Duplex: Full]
UTP   4   [Link Down     ] [Speed: -----] [Duplex: ----]
Remote A Module    [1000EAS     ]
Remote B Module    [1000EAS     ]
Port 1 OAM Mode    [Active ]
Port 2 OAM Mode    [Active ]
Advance Functions  [Normal ]

 <L> :Local    Status and Configuration.
 <A> :Remote A Status and Configuration.
 <B> :Remote B Status and Configuration.
 <M> :SNMP Manager.
 <S> :System Configuration.
```

Select item 'L' from the main menu.

From the ***Local Status and Configuration*** menu, each UTP port can be managed (activated or disabled, speed & duplex set, ingress & egress bandwidth rates set, and diagnostic loop back performed) individually per port. Select port number. Select items by number/letters.

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.240      ***
          ********************************************
<< Local Status and Configuration >>
NMC Action    [Inactive (Stand alone)]

 <1> :Fiber 1 Status and Configuration.
 <2> :Fiber 2 Status and Configuration.
 <3> :UTP   3 Status and Configuration.
 <4> :UTP   4 Status and Configuration.
 <D> :Device  Status and Configuration.
 <Q> :Static 802.1Q VLAN Status and Configuration.
 <S> :Spanning Tree Status and Configuration.
 <L> :Link Loss Forwarding Configuration.
 <C> :Counters Status and Configuration.

<ESC>:Go to Previous Menu.
```

Select the first UTP port by keying "3" at the console.

3.3.9.1 UTP Port 3 Provisioning

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.273     ***
          ******************************************
<< Local UTP 3 Status and Configuration >>
Link Status     [Link Up  ]
Speed           [100M]
Duplex          [Full]

 <1> :Port Active        [Enable ]
 <2> :Negotiation        [Auto]
 <5> :Ingress Rate Limit [Unlimited]
 <6> :Egress  Rate Limit [Unlimited]
 <7> :Default Port CoS      [0]
 <S> :Confirm and Save Settings(Port Active, Speed, Duplex and Nego

<ESC>:Go to Previous Menu.
```

<1> **Port Active** : When disabled, this port will no longer transfer any data and the link will be down.
<2> **Negotiation** : The UTP ports of this converter follow IEEE802.3u standards for n-way auto-negotiation. The port can also be manually configured, over-riding the auto-negotiation in "forced" mode. These port settings are explained in more detail under the section 3.3.9.2
<5> & <6> **Ingress/Egress Rate Limit** : These bandwidth control settings are explained in more detail under the section 3.3.9.3.
<7> **Default Port CoS** : The Class of Service is a 3 bit field within an Ethernet frame header when using 802.1Q tagging. The field specifies a priority value of between 0 and 7 inclusive that can be used by Quality of Service (QoS) disciplines to differentiate traffic. When 802.1Q is not enabled, there is no tag and therefore no 802.1p tag priority. Use this setting to set the default CoS for this port (0 to 7).
<S> **Confirm and Save Settings** : Any settings made in this menu are not saved or become active until this save procedure is completed.

3.3.9.2 UTP Port 3 Negotiation

By changing the negotiation setting from 'Auto' to 'Manual', the additional menu items 3 & 4 are revealed.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.273     ***
          ******************************************
<< Local UTP 3 Status and Configuration >>
Link Status     [Link Up  ]
Speed           [1000M]
Duplex          [Full]

 <1> :Port Active        [Enable ]
 <2> :Negotiation        [Manual]
 <3> :Speed              [1000M]
 <4> :Duplex             [Full]
 <5> :Ingress Rate Limit [Unlimited]
 <6> :Egress  Rate Limit [Unlimited]
 <7> :Use IEEE Tag's CoS    [Yes]
 <8> :Default Port CoS      [0]
 <S> :Confirm and Save Settings(Port Active, Speed, Duplex and
Negotiation).
<ESC>:Go to Previous Menu.
```

<3> **Speed** : The UTP ports support 10, 100, or 1000 forced configuration speed.
<4> **Duplex** : The UTP ports support Full or Half-Duplex operation modes. Gigabit Ethernet cannot be set to Half-Duplex as it is not standard.

3.3.9.3 UTP Port 3 Rate Limiting

The **1000EAS** provides per port ingress and egress rate limiting. For bandwidth settings, IRL or ingress rate limit refers to limiting any packets coming into the converter, while ERL or egress rate limit refers to limiting packets leaving the converter. When rate limiting is applied, ERL will use pause commands (802.3X) when the desired rate limit is exceeded, while any IRL setting will cause packet to be dropped when the limit is exceeded. This is an important point when doing the rate limit settings. It is preferable to set ERL at each port for the path that requires limiting so that flow control can help connected devices cope with the limiting. If IRL is employed, a connected device which has its packets dropped without flow control, will continue to send packets at its full rate. Also, since the packets are dropped, the application layer can only deal with the packet loss by timing out.

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.240      ***
          ********************************************
<< Local UTP 3 Status and Configuration >>
Link Status     [Link Up  ]
Speed           [1000M]
Duplex          [Full ]

 <1> :Port Active        [Enable ]
_____________________
 Select Ingress Rate Limit.

 <0> Unlimited     <1> 250M          <2> 140M          <3> 95M
 <4> 57M           <5> 40M           <6> 31M           <7> 25M
 <8> 20M           <9> 14M           <A> 10M           <B> 8M
 <C> 6M            <D> 4M            <E> 3M            <F> 2M
 <G> 1M            <H> 960K          <I> 896K          <J> 832K
 <K> 768K          <L> 705K          <M> 640K          <N> 576K
 <O> 512K          <P> 448K          <Q> 384K          <R> 320K
 <S> 256K          <T> 192K          <U> 128K          <V> 70K

<ESC>:Previous Menu.
```

The ingress rate setting menu. Select rate from 70K to 250M or unlimited.

The same setting rates can be applied to the egress direction.

3.4 Device Status and Configuration

```
          *******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          *******************************************
Fiber 1   [Link Up       ] [Remote LB: Off  ]
Fiber 2   [Link Up       ] [Remote LB: Off  ]
UTP   3   [Link Up       ] [Speed:  100M] [Duplex: Full]
UTP   4   [Link Down     ] [Speed: -----] [Duplex: ----]
Remote A Module    [1000EAS     ]
Remote B Module    [1000EAS     ]
Port 1 OAM Mode    [Active ]
Port 2 OAM Mode    [Active ]
Advance Functions  [Normal ]

 <L> :Local    Status and Configuration.
 <A> :Remote A Status and Configuration.
 <B> :Remote B Status and Configuration.
 <M> :SNMP Manager.
 <S> :System Configuration.
```

Select item 'L' from the main menu.

From the ***Local Status and Configuration*** menu, the **Device Status and Configuration** menu can view the status and set the configuration mode.

```
          *******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          *******************************************
<< Local Status and Configuration >>
NMC Action    [Inactive (Stand alone)]

 <1> :Fiber 1 Status and Configuration.
 <2> :Fiber 2 Status and Configuration.
 <3> :UTP   3 Status and Configuration.
 <4> :UTP   4 Status and Configuration.
 <D> :Device  Status and Configuration.
 <Q> :Static 802.1Q VLAN Status and Configuration.
 <S> :Spanning Tree Status and Configuration.
 <L> :Link Loss Forwarding Configuration.
 <C> :Counters Status and Configuration.

<ESC>:Go to Previous Menu.
```

Select the Device Status and Configuration by keying "D" at the console.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Local Device Status and Configuration >>
 <1> :Pause Frame        [Disable]
 <2> :Advance Functions  [Normal ]
 <3> :Maximum OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <4> :Accept Remote H/W Reset  [Disable]
 <5> :Upnp               [Disable]
 <6> :QoS Priority Mode  [Weighted]
 <7> :Tag's CoS Mapping to Internal Classify.
 <A> :Remote A H/W Reset.
 <B> :Remote B H/W Reset.
 <L> :Load Default Settings and Write to System.
 <R> :System Reboot.

<ESC>:Go to Previous Menu.
```

<1> **Pause Frame** : PAUSE is a flow control mechanism on full duplex Ethernet link segments defined by IEEE 802.3x and uses MAC Control frames to carry the PAUSE commands. Pressing the "1" key here will toggle this function between enabled or disabled.
<2> **Advanced Functions** : The 1000EAS acts as a normal 4 port switch when the setting here is 'normal'. Advanced functions are explained in detail in section 3.5.
<3> **Maximum OAMPDU Size** : This sets the maximum size of the OAM Protocol Data Unit (PDU). In order for two devices to communicate properly at the OAM level, this setting must be the same. We recommend setting the size to 1500.
<4> **Accept Remote H/W Reset** : When this parameter is enabled, the remotely connected unit will be allowed to reset this device if it gives the proper command. If this parameter is disabled (default), the remote unit's reset command will be ignored by this unit.
<5> **Upnp** : UPnP or Universal Plug 'n Play is a set of networking protocols promulgated by the UPnP Forum. When connected to a network, the **1000EAS** will automatically announce its network address and supported device and services types, enabling clients that recognize those types to immediately begin using the device.
<6>&<7> : **QoS Priority Mode** and **Tag's CoS Mapping to Internal Classify** are used to configure the Class of Service QoS in conjunction with 802.1Q VLAN. The priority mode may either be set as 'Weighted' or as 'Strict'. Note: 'Strict' mode could result in packet starvation.
<A> **Remote A H/W Reset** : This function will request the remote A unit (fiber port 1 connected unit) to do a warm boot startup. This remote unit must have enabled the "Accept Remote H/W Reset" function, or it cannot be remotely reset.
<B> **Remote B H/W Reset** : This function will request the remote B unit (fiber port 2 connected unit) to do a warm boot startup. This remote unit must have enabled the "Accept Remote H/W Reset" function, or it cannot be remotely reset.
<L> **Load Default Settings and Write to System** : This function will load all the factory default settings and write them to the internal non-volatile ram. This is equivalent to doing the "Default" factory reset with the front panel 'Default' push-button switch.
<R> **System Reboot** : The unit will undergo a 'warm boot' if this function is selected and confirmed.

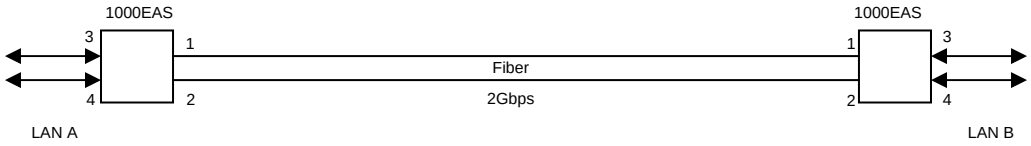
3.5 Advanced Functions

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Local Device Status and Configuration >>
 <1> :Pause Frame        [Disable]
 <2> :Advance Functions  [Normal ]
 <3> :Maximum OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <4> :Accept Remote H/W Reset  [Disable]
_____________________________________________________________________
 Select Advance Functions.

 <0> Normal
 <1> Port 1 and Port 2 Trunk Bandwidth 2G
 <2> Port 1 to Port 2 Mirror
 <3> Port VLAN(1/3; 2/4)
 <4> Port 1 and Port 2 Redundancy
 <5> Static 802.1Q VLAN
 <6> Static 802.1Q VLAN & Port 1/2 Redundancy
 <7> 802.1Q VLAN Trunk
 <8> Spanning Tree Protocol

<ESC>:Previous Menu.
```

The **1000EAS** has several sets of pre-defined 'advanced functions' which allow the user to quickly configure the switch for specific applications. Each of these is shown below and will be explained in detail.

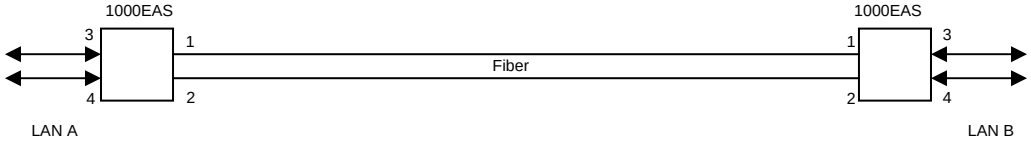
<0> **Normal** : This is the default mode of the **1000EAS**. In this mode the unit is simply a 4 port managed media converter/switch.
<1> **Port 1 and Port 2 Trunk Bandwidth 2G** : This mode creates a 2G trunk of the two 1GbE fibers by using Link Aggregation. The application drawing for this mode is shown in section 3.5.1.
<2> **Port 1 to Port 2 Mirror** : The port mirroring function is typically used by network engineers that require capturing packet data for analysis or troubleshooting. The application drawing for this mode is shown in section 3.5.2.
<3> **Port VLAN(1/3; 2/4)** : This function will allow the media converter/switch to act like two separate gigabit media converters. By using port based VLAN, traffic is isolated between the port pairs 1 and 3 and 2 and 4. The application drawing for this mode is shown in section 3.5.3.
<4> **Port 1 and Port 2 Redundancy** : This function provides a fiber redundancy so that if either fiber path losses transmission, the other path is a backup. The application drawing for this mode is shown in section 3.5.4.
<5> **Static 802.1Q VLAN** : This mode will open up the unit to further settings for 802.1Q VLAN settings. This mode's application drawing and details are shown in section 3.5.5.
<6> **Static 802.1Q VLAN & Port 1/2 Redundancy** : This special mode combines fiber port redundancy with tagged VLAN. The application drawing and details for this mode are shown in section 3.5.6.
<7> **802.1Q VLAN Trunk** : This is a special mode designed for connecting a **1000EAS** pair on the 'trunk' between Cisco switches. The application drawing and details for this mode are shown in section 3.5.7.
<8> **Spanning Tree Protocol** : The Spanning tree protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. Use this protocol when setting up the converter/switch in ring or mesh topologies. The application drawing and details for this mode are shown in section 3.5.8.

3.5.1 Port 1 and Port 2 Trunk Bandwidth 2G



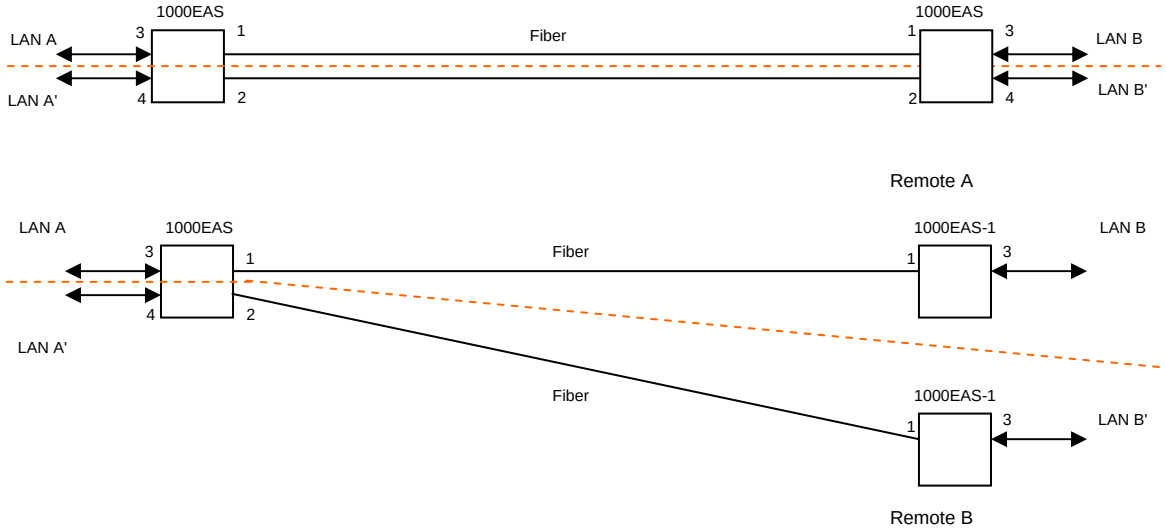
In this mode the fibers are aggregated or 'trunked' to provide 2G bandwidth. The application requires two fiber links at the same time, but logically they act as one link with up to 2G throughput. This mode can provide up to 1G throughput for each of the UTP ports at the same time.

3.5.2 Port 1 to Port 2 Mirror



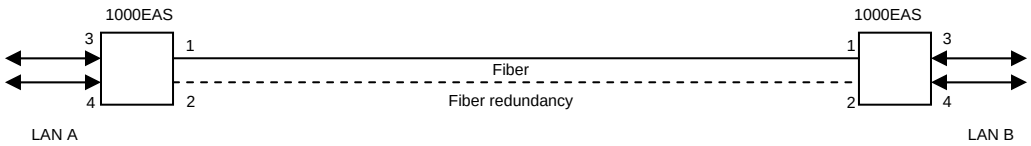
The mirror mode provides fiber aggregation or 'trunking'. It uses one or two fiber lines to achieve this feature. The maximum combined throughput is about 1.5G.

3.5.3 Port VLAN (1/3; 2/4)



The single **1000EAS** acts like two gigabit media converters in one package. The centrally located converter may also connect to two different remote locations with **1000EAS-1** at each remote, as shown in the second graphic above.

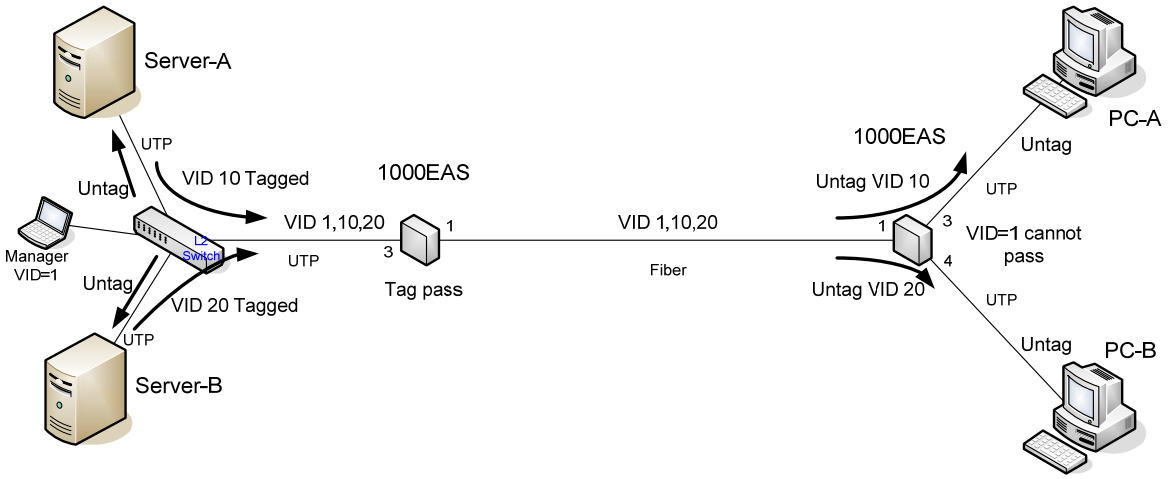
3.5.4 Port 1 and Port 2 Redundancy



In this mode one fiber is active, while the other is on standby. This creates a 1+1 redundant path protection. If main fiber is broken, the second fiber will quickly take over the transmissions. The application requires two fiber links at the same time, but one fiber is in standby.

3.5.5 Static 802.1Q VLAN

IEEE 802.1Q, or VLAN (Virtual LAN) Tagging, is a networking standard written by the IEEE 802.1 workgroup allowing multiple bridged networks to transparently share the same physical network link without leakage of information between networks.



In the above example, a L2 switch creates two separate VLANs (VID10 and VID20) from two ports that link to servers A and B. A third port carries the two VLAN IDs to the **1000EAS** media converter /switch pair by UTP. The management uses VID=1. The **1000EAS** pair creates a fiber link over a longer distance than could be supported with UTP. The local side converter requires no additional configuration and passes the tag information transparently over the fiber link. The remote side requires VLAN configuration. One UTP port (port3) recognizes and untags VID10 to the client PC-A. The other UTP port, (port4) recognizes and untags VID20 to the client PC-B. On the return trip, packets are tagged, VID10 for port3 and VID20 for port 4 and returned to the L2 switch and then to the appropriate servers.

Configuration example, done to remote converter:

1. Return to the main menu on the local unit.

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.240      ***
          ********************************************
Fiber 1   [Link Up       ] [Remote LB: Off  ]
Fiber 2   [Link Up       ] [Remote LB: Off  ]
UTP   3   [Link Up       ] [Speed:  100M] [Duplex: Full]
UTP   4   [Link Down     ] [Speed: -----] [Duplex: ----]
Remote A Module    [1000EAS     ]
Remote B Module    [1000EAS     ]
Port 1 OAM Mode    [Active ]
Port 2 OAM Mode    [Active ]
Advance Functions  [Normal ]

 <L> :Local    Status and Configuration.
 <A> :Remote A Status and Configuration.
 <B> :Remote B Status and Configuration.
 <M> :SNMP Manager.
 <S> :System Configuration.

<ESC>:Logout.
```

2. Select item <A> to go to **Remote A Status and Configuration**.

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.240      ***
          ********************************************
<< Remote A Status and Configuration >>
Firmware Version     [3.240]
Remote NMC Action    [Inactive (Stand alone)]

 <1> :Fiber 1 Status and Configuration.
 <2> :Fiber 2 Status and Configuration.
 <3> :UTP   3 Status and Configuration.
 <4> :UTP   4 Status and Configuration.
 <D> :Device  Status and Configuration.
 <Q> :Static 802.1Q VLAN Status and Configuration.
 <S> :Spanning Tree Status and Configuration.
 <L> :Link Loss Forwarding Configuration.
 <C> :Counters Status and Configuration.
 <U> :Upgrade F/W of Remote device by OAM.

<ESC>:Go to Previous Menu.
```

3. Select <D>, **Device Status and Configuration**
The screen will look like the following.

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.240      ***
          ********************************************
<< Remote A Device Status and Configuration >>
 <1> :Pause Frame        [Disable]
 <2> :Advance Functions  [Normal ]
 <3> :Maximum OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <4> :Accept Remote H/W Reset  [Disable]
 <5> :Upnp               [Disable]
 <L> :Load Default Settings and Write to System.
 <R> :System Reboot.

<ESC>:Go to Previous Menu.
```

4. Select <2>, **Advanced Functions**
The screen will look like the following.

```
Select Advance Functions.

 <0> Normal
 <1> Port 1 and Port 2 Trunk Bandwidth 2G
 <2> Port 1 to Port 2 Mirror
 <3> Port VLAN(1/3; 2/4)
 <4> Port 1 and Port 2 Redundancy
 <5> Static 802.1Q VLAN
 <6> Static 802.1Q VLAN & Port 1/2 Redundancy
 <7> 802.1Q VLAN Trunk
 <8> Spanning Tree Protocol

<ESC>:Previous Menu.
```

5. From the Advanced Functions screen, select <5> **Static 802.1Q VLAN**. The following screen will be displayed.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Remote A Device Status and Configuration >>
 <1> :Pause Frame        [Disable]
 <2> :Advance Functions  [Static 802.1Q VLAN]
 <3> :Maximun OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <4> :Accept Remote H/W Reset  [Disable]
 <5> :Upnp               [Disable]
 <L> :Load Default Settings and Write to System.
 <R> :System Reboot.

<ESC>:Go to Previous Menu.
```

6. Now leave this screen by pressing ESC. This will take us back to the **Status and Configuration** page.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Remote A Status and Configuration >>
Firmware Version     [3.240]
Remote NMC Action    [Inactive (Stand alone)]

 <1> :Fiber 1 Status and Configuration.
 <2> :Fiber 2 Status and Configuration.
 <3> :UTP   3 Status and Configuration.
 <4> :UTP   4 Status and Configuration.
 <D> :Device  Status and Configuration.
 <Q> :Static 802.1Q VLAN Status and Configuration.
 <S> :Spanning Tree Status and Configuration.
 <L> :Link Loss Forwarding Configuration.
 <C> :Counters Status and Configuration.
 <U> :Upgrade F/W of Remote device by OAM.

<ESC>:Go to Previous Menu.
```

7. Select <Q>, **Static 802.1Q VLAN Status and Configuration**
The screen will look like that on the following page.

Some Tagging definitions:
Tagged: This means that packets exiting the assigned port will have the packets tagged with the VID assigned to that port.
Untagged: This means that any packets exiting the assigned port will have all tag information removed.
Non-member: When a port is not a member of a VID, packets tagged with that VID will not be allowed to exit that port.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Remote A Static 802.1Q VLAN status and Configuration >>
Port 1:
      <1> :VID          [      1]     <2> :Tag Priority [  0]
      <3> :QinQ Support [Disable]     <4> :Use Tag Type [No ]
Port 2:
      <5> :VID          [      1]     <6> :Tag Priority [  0]
      <7> :QinQ Support [Disable]     <8> :Use Tag Type [No ]
Port 3:
      <A> :VID          [      1]     <B> :Tag Priority [  0]
      <C> :QinQ Support [Disable]     <D> :Use Tag Type [No ]
Port 4:
      <E> :VID          [      1]     <F> :Tag Priority [  0]
      <G> :QinQ Support [Disable]     <H> :Use Tag Type [No ]
 <M> :Management VID [   1]
 <T> :Tag Type (Hex) [8100]
 <Z> :Go to VLAN Table Configuration Page.
 <S> :Save Settings.

<ESC>:Don't Save Settings and Go to Previous Menu.
```

In the above table, we can set different VID (VLAN Identifier) for each port of the converter. QinQ support can also be enabled. Double-tagging (QinQ) can be useful for Internet Service Providers, allowing them to use VLANs internally while mixing traffic from clients that are already VLAN-tagged. The outer (representing ISP VLAN) tag comes first, followed by the inner tag. In such cases, an alternate TPID such as hex 9100 may be used for the outer tag; however this is being deprecated by 802.1ad, which specifies 88a8 for service-provider outer tags.

8. We are going to set port 3 (UTP3) to VID 10 and port 4 (UTP4) to VID20. The screen will then look like this. This means that packets that ingress (come into) the UTP ports, from PC-A and PC-B will have their packets tagged for VID10 and 20 respectively. Save settings with <S>.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Remote A Static 802.1Q VLAN status and Configuration >>
Port 1:
      <1> :VID          [      1]     <2> :Tag Priority [  0]
      <3> :QinQ Support [Disable]     <4> :Use Tag Type [No ]
Port 2:
      <5> :VID          [      1]     <6> :Tag Priority [  0]
      <7> :QinQ Support [Disable]     <8> :Use Tag Type [No ]
Port 3:
      <A> :VID          [     10]     <B> :Tag Priority [  0]
      <C> :QinQ Support [Disable]     <D> :Use Tag Type [No ]
Port 4:
      <E> :VID          [     20]     <F> :Tag Priority [  0]
      <G> :QinQ Support [Disable]     <H> :Use Tag Type [No ]
 <M> :Management VID [   1]
 <T> :Tag Type (Hex) [8100]
 <Z> :Go to VLAN Table Configuration Page.
 <S> :Save Settings.

<ESC>:Don't Save Settings and Go to Previous Menu.
```

9. Next we need to go to the **VLAN Table Configuration Page**. Select item <Z>.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Remote A Static VLAN Table Configuration >>
  Item |  VLAN ID  |   Port 1   |   Port 2   |   Port 3   |
Port 4









 <N><PageDown>:Show Next Page.
 <P><PageUp>  :Show Previous Page.
 <DownArrow>:Show Next Item.
 <UpArrow>  :Show Previous Item.
 <V> :VLAN Table Operation.
 <R> :Reset Static 802.1Q VLAN Settings.
 <C> :Clear Static 802.1Q VLAN Table.

<ESC>:Go to Port VID Configuration Page..
```

The static **VLAN table Operation** is accessed through the **<V>** menu item.

10. Select <V> **VLAN Table Operation**.

```
Operate:[      ]

.....................................................................
 Operate VLAN Table: Select Operation.
 <1> Modify         <2> Create         <3> Delete

<ESC>:Discard and Return.
```

In our example, Port 1 is the fiber port or the main WAN link. Ports 3&4 are UTP ports. We will assign static VLAN to VID1, 10, and 20 as follows.

11. Select <2> **Create**. Input the VID 1

```
Operate:[Create]    VLAN ID:[    ]

.....................................................................
 Operate VLAN Table: Select VLAN ID.

<ESC>:Previous Page.

Please Input 1 ~ 4094 :[   1]
```

12. For VID 1 we will select the port membership in order for Port 1, Port 2, Port3 and Port 4 as 'untagged', 'nonmember', 'nonmember', and 'nonmember'.

```
Operate:[Create]    VLAN ID:[   1]
 Port 1:[          ],Port 2:[          ],Port 3:[          ],Port 4:[          ]
.....................................................................
 Operate VLAN Table: Select Port 1 Membership.
 <1> UnModified     <2> UnTagged       <3> Tagged         <4> NonMember

<ESC>:Previous Page.
```

The results look like this.

```
           ******************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
           ***      FRM220-1000EAS     Ver:3.240     ***
           ******************************************
<< Remote A Static VLAN Table Configuration >>
 Item |  VLAN ID  |   Port 1   |   Port 2   |   Port 3   |   Port 4
  01  |      1    |  Untagged  |  Nonmember |  Nonmember |  Nonmember
```

By making Port3&4 nonmembers of VID1, we have blocked any normal traffic between those two clients. They are isolated from each other.

The next step will be to create the VIDs for 10 and 20. We will make Port3&4 untagged members of VID10 and 20 respectively. Port 1 (fiber) will be Tagged member for each VLAN.

The resulting Static VLAN table will look like this:

```
           ******************************************
           ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
           ***      FRM220-1000EAS     Ver:3.240     ***
           ******************************************
<< Remote A Static VLAN Table Configuration >>
 Item |  VLAN ID  |   Port 1   |   Port 2   |   Port 3   |   Port 4
  01  |      1    |  Untagged  |  Nonmember |  Nonmember |  Nonmember
  02  |     10    |   Tagged   |  Nonmember |  Untagged  |  Nonmember
  03  |     20    |   Tagged   |  Nonmember |  Nonmember |  Untagged



 <N><PageDown>:Show Next Page.
 <P><PageUp>  :Show Previous Page.
 <DownArrow>:Show Next Item.
 <UpArrow>  :Show Previous Item.
 <V> :VLAN Table Operation.
 <R> :Reset Static 802.1Q VLAN Settings.
 <C> :Clear Static 802.1Q VLAN Table.

<ESC>:Go to Port VID Configuration Page.
```

This simple VLAN scheme will now be working such that PC-A can only connect to Server A and PC-B can only connect to Server B.

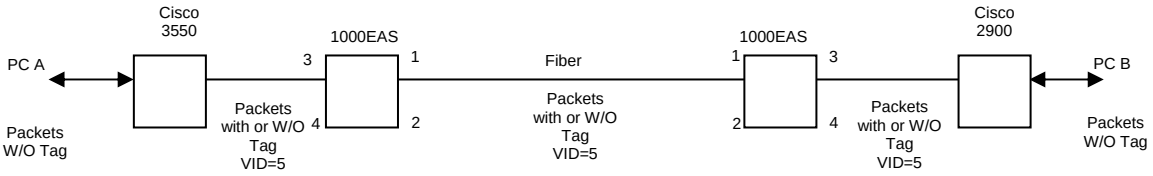
When assigning static VLAN ID, any ID from 1-4094 can be chosen. However, the maximum number of VID table entries for the **1000EAS** is 64 static VLANs.

3.5.6 Static 802.1Q VLAN & Port 1/2 Redundancy

By choosing the **Advanced Feature** of Static VLAN and Port Redundancy, the previous application in section 3.5.5 with VLAN can be combined with section 3.5.4 Port 1 + Port 1 fiber redundancy.

3.5.7 802.1Q VLAN Trunk

The **VLAN Trunk** feature is a quick way to configure the **1000EAS** for management between two trunked Cisco switches. In the following application, the existing trunk VLAN is already provided between the two Cisco switches. The object here is to be able to allow the PC at either end (PC-A or PC-B) to manage the **1000EAS** devices. In this example, the management VID=5.



The above application configuration can be done manually through the normal 802.1Q setting menus. First we will explain the manual setting mode.

From the main menu, select either the Local or Remote A unit for configuration. Select <Q> for 802.1Q setting.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.273     ***
          ******************************************
<< Remote A Static 802.1Q VLAN status and Configuration >>
Port 1:
  Priority for Tag [CoS 0]
  <1> :VID  [   1]    <2> :QinQ Support [Disable]    <3> :Use Tag Type [No ]
Port 2:
  Priority for Tag [CoS 0]
  <4> :VID  [   1]    <5> :QinQ Support [Disable]    <6> :Use Tag Type [No ]
Port 3:
  Priority for Tag [CoS 0]
  <7> :VID  [   1]    <8> :QinQ Support [Disable]    <9> :Use Tag Type [No ]
Port 4:
  Priority for Tag [CoS 0]
  <A> :VID  [   1]    <B> :QinQ Support [Disable]    <C> :Use Tag Type [No ]
 <M> :Management VID [   1]
 <T> :Tag Type (Hex) [8100]
 <Z> :Go to VLAN Table Configuration Page.
 <S> :Save Settings.

<ESC>:Don't Save Settings and Go to Previous Menu
```

Select <M> **Management VID** and change to 5. Save.

```
 Set Management VID(The Default Value of 1).

<ESC>:Discard and Return.

Please Input 1 ~ 4094 :[5   ]
```

Next, configure the Static 802.1Q VLAN table as follows:

1. Make VID=1 and 'Untag' for all ports.
2. Make VID=5 and make it 'Tagged' for port 1 (fiber) and 'Tagged' for port 3 (UTP). You can set ports 2 & 4 to 'Untagged' if they are not used.

From the VLAN Status and Configuration page, select <Z> **Go to VLAN Table Configuration**. Then select <V> **VLAN Table Operation**. Create VID 1 and untag all ports. Save. The create VID 5 and make sure it is 'Tagged' on ports 1 and 3. Save

The results look like this:

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.273     ***
          ******************************************
<< Remote A Static VLAN Table Configuration >>
  Item |  VLAN ID  |   Port 1   |   Port 2   |   Port 3   |   Port 4
   01  |      1    |  Untagged  |  Untagged  |  Untagged  |  Untagged
   02  |      5    |   Tagged   |  Untagged  |   Tagged   |  Untagged




 <N><PageDown>:Show Next Page.
 <P><PageUp>  :Show Previous Page.
 <DownArrow>:Show Next Item.
 <UpArrow>  :Show Previous Item.
 <V> :VLAN Table Operation.
 <R> :Reset Static 802.1Q VLAN Settings.
 <C> :Clear Static 802.1Q VLAN Table.

<ESC>:Go to Port VID Configuration Page.
```

Now, PC-A and PC-B can both manage the **1000EAS**. PC-A can ping PC-B.

To do all the above without any other settings, simply choose the **<7> 802.1Q VLAN Trunk** Advanced Feature, from the **Device Status and Configuration** page and set the Management VID=5. All other settings will be automatically done.

Action performed by this application:

If an untagged packet ingresses at **1000EAS** port 1 (Fiber), VID=1 tag will be added to the packet from the switch. When the packet egresses port 3 (UTP) VID=1 tag will be removed (untagged).

If a tagged packet with VID=5 ingresses at **1000EAS** port 1 (Fiber), it will be passed through the internal switch and still be tagged with VID=5 as it egresses port 3 (UTP).

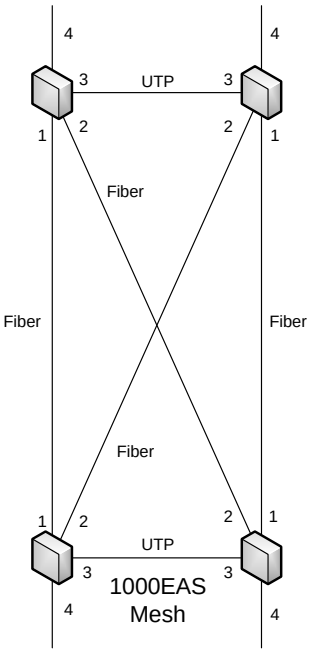
3.5.8 Spanning Tree Protocol

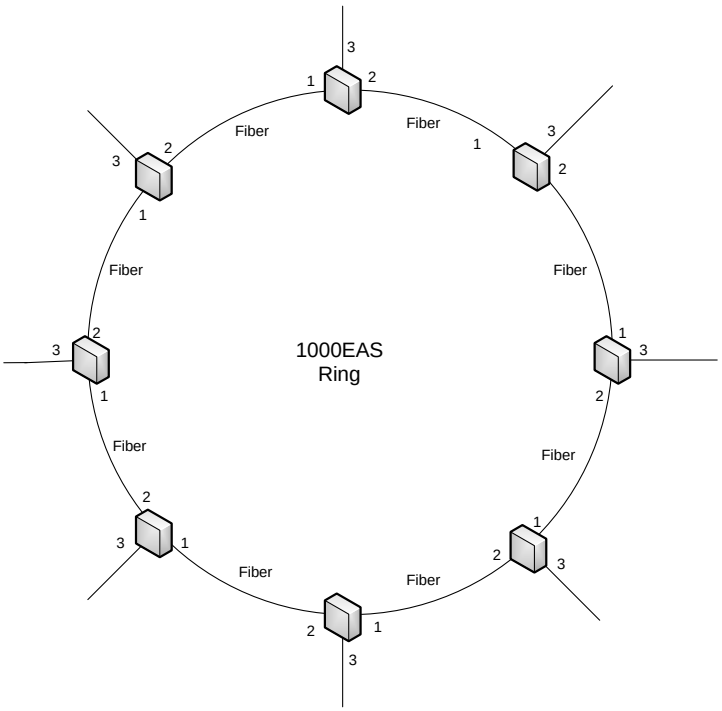
The Spanning Tree Protocol (STP) is a link layer (OSI Layer 2) network protocol that ensures a loop-free topology for any bridged LAN. The basic function of STP is to prevent bridge loops and ensuing broadcast radiation.

STP is standardized as 802.1D. It creates a spanning tree within a mesh network of connected layer-2 Ethernet switches, and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.

Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. Bridge loops must be avoided because they result in flooding the internet network.

The following two examples that use STP are the ring and mesh topologies. Redundancy is built into these topologies as Mesh and Ring networks are self-healing through STP.





1. Return to the main menu on the local unit.

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.240      ***
          ********************************************
Fiber 1   [Link Up       ] [Remote LB: Off  ]
Fiber 2   [Link Up       ] [Remote LB: Off  ]
UTP   3   [Link Up       ] [Speed:  100M] [Duplex: Full]
UTP   4   [Link Down     ] [Speed: -----] [Duplex: ----]
Remote A Module    [1000EAS     ]
Remote B Module    [1000EAS     ]
Port 1 OAM Mode    [Active ]
Port 2 OAM Mode    [Active ]
Advance Functions  [Normal ]

 <L> :Local    Status and Configuration.
 <A> :Remote A Status and Configuration.
 <B> :Remote B Status and Configuration.
 <M> :SNMP Manager.
 <S> :System Configuration.

<ESC>:Logout.
```

2. Select the **local unit** for configuration by choosing **<L>**.

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.240      ***
          ********************************************
<< Local Status and Configuration >>
NMC Action    [Inactive (Stand alone)]

 <1> :Fiber 1 Status and Configuration.
 <2> :Fiber 2 Status and Configuration.
 <3> :UTP   3 Status and Configuration.
 <4> :UTP   4 Status and Configuration.
 <D> :Device  Status and Configuration.
 <Q> :Static 802.1Q VLAN Status and Configuration.
 <S> :Spanning Tree Status and Configuration.
 <L> :Link Loss Forwarding Configuration.
 <C> :Counters Status and Configuration.

<ESC>:Go to Previous Menu.
```

3. Select the **Device Status and Configuration** menu by choosing **<D>**.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Local Device Status and Configuration >>
 <1> :Pause Frame        [Disable]
 <2> :Advance Functions  [Normal ]
 <3> :Maximun OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <4> :Accept Remote H/W Reset  [Disable]
 <5> :Upnp               [Disable]
 <A> :Remote A H/W Reset.
 <B> :Remote B H/W Reset.
 <L> :Load Default Settings and Write to System.
 <R> :System Reboot.

<ESC>:Go to Previous Menu.
```

4. Select the **Advanced Functions** menu by choosing **<2>**.

```
Select Advance Functions.

 <0> Normal
 <1> Port 1 and Port 2 Trunk Bandwidth 2G
 <2> Port 1 to Port 2 Mirror
 <3> Port VLAN(1/3; 2/4)
 <4> Port 1 and Port 2 Redundancy
 <5> Static 802.1Q VLAN
 <6> Static 802.1Q VLAN & Port 1/2 Redundancy
 <7> 802.1Q VLAN Trunk
 <8> Spanning Tree Protocol

<ESC>:Previous Menu.
```

5. Esc back to the **Local Status and Configuration** menu

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Local Status and Configuration >>
NMC Action    [Inactive (Stand alone)]

 <1> :Fiber 1 Status and Configuration.
 <2> :Fiber 2 Status and Configuration.
 <3> :UTP   3 Status and Configuration.
 <4> :UTP   4 Status and Configuration.
 <D> :Device  Status and Configuration.
 <Q> :Static 802.1Q VLAN Status and Configuration.
 <S> :Spanning Tree Status and Configuration.
 <L> :Link Loss Forwarding Configuration.
 <C> :Counters Status and Configuration.

<ESC>:Go to Previous Menu.
```

6. Select **<S>**. to bring up the **Spanning Tree Status and Configuration** menu.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Local Spanning Tree Status >>
Bridge Status:
  STP Enable       [ON               ]     Bridge ID      [8000.0002abfffe02]
  Designated Root  [8000.0002abfffe02]     Root Port      [0                 ]
  Root Path Cost   [0                ]     Max Age        [20                ]
  Hello Time       [2                ]     Forward Delay  [15                ]

Port 1 Status:
  Bridge Port      [Yes              ]     Port ID        [8001              ]
  Port State       [Forwarding       ]     Path Cost      [4                 ]
  Designated Bridge[8000.0002abfffe02]     Designated Port[8001              ]

 <P><LeftArrow> :Previous Port.
 <N><RightArrow>:Next Port.
 <G> :Go to STP Configuration Menu.

<ESC>:Previous Menu.
```

The root bridge of the spanning tree is the bridge with the lowest bridge ID. Each bridge has a unique identifier (ID) and a configurable priority number; the **Bridge ID** contains both numbers. To compare two bridge IDs, the priority is compared first. If two bridges have equal priority, then the MAC addresses are compared. For example, if switches A (MAC=0002abfffe02) and B (MAC=0002abfffe03) both have a priority of 8000, then switch A will be selected as the root bridge (it has the lower value MAC address). If the network administrators would like switch B to become the root bridge, they must set its priority to be less than 8000.

Spanning tree computes its path by following the path of least cost, i.e., a path from the device to the root that has minimum cost among all paths from the device to the root. The cost of traversing a path is the sum of the costs of the segments on the path. The port connecting to that path becomes the root port (RP) of the bridge. Different technologies have different default costs for network segments. An administrator can configure the cost of traversing a particular network segment. The default **root path cost** in the **1000EAS** is 0.

The switch sends a **BPDU** (Bridge Protocol Data Units) frame using the unique MAC address of the port itself as a source address, and a destination address of the STP multicast address 01:80:C2:00:00:00.

There are three types of BPDUs:

1. Configuration BPDU (CBPDU), used for Spanning Tree computation
2. Topology Change Notification (TCN) BPDU, used to announce changes in the network topology
3. Topology Change Notification Acknowledgment (TCA)

Hello Time is the time interval (number of seconds between) at which the root bridge transmits configuration BPDUs.

When a device is first attached to a switch port, it will not immediately start to forward data. It will instead go through a number of states while it processes BPDUs and determines the topology of the network. The time spent in the listening and learning states is determined by a value known as the **forward delay** (default 15 seconds and set by the root bridge).

Maximum Age, referred to by the switch as **Max Age**, is the amount of time a switch will retain a BPDU's contents before discarding it. The default is 20 seconds. It also influences the bridge table aging timer during the Topology Change Notification process.

Remember that these timers should not be changed lightly. If you decide to change any or all of these timers, that change must be configured on the root bridge! The root bridge will inform the nonroot switches of the change via BPDUs.

3.5.9 Class of Service

Class of Service (COS) is a technique used to deliver Quality of Service (QoS) in a network. CoS is a way of classifying and prioritizing packets based on classification. A "first class" priority label is assigned to data applications - such as mission-critical data transactions, or video or voice transmissions - which require faster turnaround, while a lower-priority label is assigned to less time-sensitive traffic, such as e-mail and Web surfing.

CoS, as defined in IEEE 802.1p, uses Layer 2 VLAN Tagging and makes use of three bits in the Ethernet frame header that can be used to specify priority. The field specifies a priority value of between 0 and 7 inclusive that can be used by Quality of Service (QoS) disciplines to differentiate traffic.

CoS operates only on Ethernet at the data link layer.

Where QoS mechanisms are used, an aggregate traffic stream may be classified into a number of constituent classes, and different QoS guarantees may be provided to different classes within the aggregate. When a class has a defined minimum bandwidth assurance, this is referred to as the ***class capacity***.

The **1000EAS** supports either a fixed-priority (strict-priority) or weighted (fair-queuing) scheme.

In the strict priority scheme, all top-priority frames egress a port until that priority's queue is empty. Then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures all high priority frames egress the switch as soon as possible.

In the weighted scheme, an 8, 4, 2, 1 weighting is applied to the four queue priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.

The IEEE 802.3ac Tag contains IEEE 802.1p priority information, and it will override any default port CoS policy.

The switch in the **1000EAS** has four internal priority queues (0~3) which need to be mapped to the 802.1Q QoS eight priority (0~7) levels. The switch requires that each port (two fiber and two UTP in the 1000EAS) have a mapping for queue priority.

To configure the CoS feature, first, from the main menu go to the <L> **Local Status and Configuration** menu, then select <D> **Device Status and Configuration**, then select <7> **Tag's CoS Mapping to Internal Classify**. This is where the Class of Service priority (0~7) can be mapped to the 1000EAS internal switch's priority queues (0~3). In the switch, 3 is the highest priority queue and 0 has the lowest priority.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.    ***
          ***      FRM220-1000EAS     Ver:3.273     ***
          ******************************************
<< Tag CoS Mapping to Internal Classify >>

 <1> :CoS 0  [1]
 <2> :CoS 1  [0]
 <3> :CoS 2  [0]
 <4> :CoS 3  [1]
 <5> :CoS 4  [2]
 <6> :CoS 5  [2]
 <7> :CoS 6  [3]
 <8> :CoS 7  [3]

<ESC>:Go to Previous Menu.
```

From the **Device Status and Configuration** page, the egress scheduling can be configured either as a weighted classification or as strict classification.

```
Set Egress Scheduling Mode.

 <1> Weighted          <2> Strict

<ESC>:Previous Menu.
```

Next, for each of the **1000EAS** ports (two fiber and two UTP) the CoS priority is assigned.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.273     ***
          ******************************************
<< Local Fiber 1 Status and Configuration >>
Link Status              [Link Up  ]
Remote Device Power      [OK]
OAM Remote Loopback Test [OFF]
OAM Looped               [OFF]

 <1> :Port Active           [Enable ]
 <2> :Auto Laser Shutdown   [Disable]
 <3> :OAM Channel A Mode    [Active ]
 <4> :Remote Loopback Test  [Disable]
 <5> :Ingress Rate Limit    [Unlimited]
 <6> :Egress  Rate Limit    [Unlimited]
_____________________________________________________________________________
 Set Default Port's Class of Service(CoS).

 <0> 0          <1> 1          <2> 2          <3> 3
 <4> 4          <5> 5          <6> 6          <7> 7

<ESC>:Previous Menu.
```

So, for example, if the fiber port's CoS is set to '7' and CoS priority 7 is mapped to the internal switch's queue 3, then packets destined to egress this fiber port will have the highest priority.

To disable the CoS feature for this port, select <7> :Use IEEE Tag's CoS [Yes] and toggle the the value to 'No'.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.273     ***
          ******************************************
<< Local Fiber 1 Status and Configuration >>
Link Status              [Link Up  ]
Remote Device Power      [OK]
OAM Remote Loopback Test [OFF]
OAM Looped               [OFF]

 <1> :Port Active           [Enable ]
 <2> :Auto Laser Shutdown   [Disable]
 <3> :OAM Channel A Mode    [Active ]
 <4> :Remote Loopback Test  [Disable]
 <5> :Ingress Rate Limit    [Unlimited]
 <6> :Egress  Rate Limit    [Unlimited]
 <7> :Use IEEE Tag's CoS    [No ]
 <8> :Default Port CoS      [7]
 <S> :SFP and D/D Function  [Yes]

<ESC>:Go to Previous Menu.
```

3.6 OAM Configuration

Ethernet in the First Mile (**EFM**) is the nickname of IEEE Std 802.3ah-2004, an amendment to the Ethernet standard, specifying "Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks". The EFM standard was approved by the IEEE Standards Board in June 2004, and officially published on September 7, 2004. In 2005 it was included into the base IEEE 802.3 standard.

The "Last Mile" is the name traditionally given to the part of a public communication network that links the last provider-owned node (the central office, the street cabinet or pole) with the customer premises equipment (CPE). The "First Mile" is the exact same thing, viewed from the customer's perspective.

IEEE 802.3ah **OAM** (Operations, Administration, Maintenance) specification covers the OAM frames used across a physical IEEE 802.3 medium between a Provider and a Customer, or perhaps between two Provider ports or two Customer ports. In the **1000EAS** product, OAM refers to the frames sent between units over fiber links. OAM is **NOT** forwarded over links.

Ethernet **OAM** is complementary, not competitive, with **SNMP** (Simple Network Management Protocol) management in that it provides some basic management functions at layer two, rather than using layer three and above as required by SNMP over an IP infrastructure. Ethernet OAM provides single-hop functionality in that it works only between two directly connected Ethernet stations. SNMP can be used to manage the Ethernet OAM interactions of one Ethernet station with another.

3.6.1 OAM PDU frame size

OAM PDU frames must be within the legal Ethernet frame size range of 64 to 1518 bytes. OAM frames **MUST** be untagged. The maximum transmit rate of OAM PDU frames is 10 per second. In an OAM pair, only the 'Active' unit needs to set the frame size. The 'Passive' OAM unit will negotiate and follow the 'Active' unit during **OAM Discovery**. The default and recommended OAM PDU size is 1500 bytes. The active and passive units must have the same OAM frame size.

To configure, from the main menu, select <L> (Local Status and Configuration), then select <D> (Device Status and Configuration). From this menu select <3> (Maximum OAMPDUs Size) and set as follows.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Local Device Status and Configuration >>
 <1> :Pause Frame        [Disable]
 <2> :Advance Functions  [Spanning Tree Protocol]
 <3> :Maximun OAMPDUs Size (60 ~ 1518 Octets) [1500]
 <4> :Accept Remote H/W Reset  [Disable]
 <5> :Upnp               [Disable]
 <A> :Remote A H/W Reset.
 <B> :Remote B H/W Reset.
 <L> :Load Default Settings and Write to System.
 <R> :System Reboot.

<ESC>:Go to Previous Menu.
_____________________________________________________________________
 Set MAX OAMPDUs Size(Allowed Range: 60 ~ 1518 Bytes).

<ESC>:Discard and Return.

Please Input Size:[1518]
```

3.6.2 OAM Mode

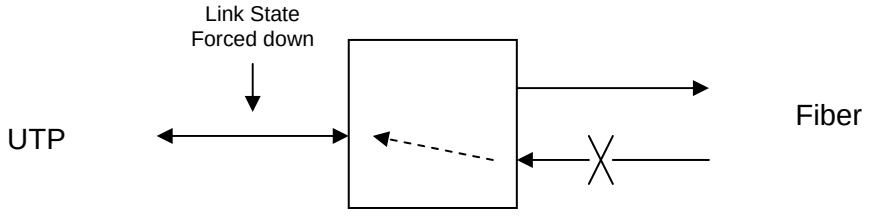
The OAM in the **1000EAS** converter only works on fiber links. Both units on the fiber link must be CTC Union **1000EAS** family units. The OAM mode can be set to one of three choices: disabled, active or passive. In the OAM scheme, the 'active' unit will provide the OAM configuration to 'passive' unit during OAM discovery phase. If both units on the fiber link are set to 'active' mode, the one with lower MAC address will become the active node and the higher MAC address unit will assume passive mode.

To configure, from the main menu, select <L> (Local Status and Configuration), then select the fiber port (1 or 2) <1> (Local Fiber 1 Status and Configuration). From this menu select <3> (OAM Channel A Mode) and set as follows.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< Local Fiber 1 Status and Configuration >>
Link Status              [Link Up  ]
Remote Device Power      [OK]
OAM Remote Loopback Test [OFF]
OAM Looped               [OFF]

 <1> :Port Active           [Enable ]
 <2> :Auto Laser Shutdown   [Disable]
 <3> :OAM Channel A Mode    [Active ]
 <4> :Remote Loopback Test  [Disable]
 <5> :Ingress Rate Limit    [Unlimited]
 <6> :Egress  Rate Limit    [Unlimited]
 <S> :SFP and D/D Function  [Yes]
_____________________________________________________________________________
 Set OAM Mode.

 <0> Disable        <1> Passive        <2> Active

<ESC>:Previous Menu.
```

3.7 Link Loss Forwarding

In a simple media converter (two ports), a loss of fiber receive signal (link failure) can be used to force down the electrical Ethernet link and visa versa. This mechanism is referred to as "Link Loss Forwarding" or "Link Fault Pass-thru".



Link Loss Forwarding (LLF) Mechanism

The **1000EAS** model is a four port L2 Gigabit Ethernet switch with two fiber and two electrical Ethernet ports. With Link Loss Forwarding mechanism, when one Ethernet port detects a link down condition, this media converter can be programmed to logically force down any or all of the other Ethernet ports. The settings are done by check box in a 4x4 matrix.

To configure, from the main menu, select <L> (Local Status and Configuration), then select <L> (Link Loss Forwarding Configuration).

```
          ****************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ****************************************
<< Local Link Loss Forwarding Configuration >>
                            |                Condition                |
                            |  Port 1  |  Port 2  |  Port 3  |  Port 4  |
                | Logical   | Link Loss| Link Loss| Link Loss| Link Loss|
----------------+-----------+----------+----------+----------+----------|
Port 1 Power Off | <0>[AND] |          |  <1>[ ]  |  <2>[ ]  |  <3>[ ]  |
----------------+-----------+----------+----------+----------+----------|
Port 2 Power Off | <4>[AND] |  <5>[ ]  |          |  <6>[ ]  |  <7>[ ]  |
----------------+-----------+----------+----------+----------+----------|
Port 3 Power Off | <8>[AND] |  <9>[ ]  |  <A>[ ]  |          |          |
----------------+-----------+----------+----------+----------+----------|
Port 4 Power Off | <B>[AND] |  <C>[ ]  |  <D>[ ]  |          |          |
----------------+-----------+----------+----------+----------+----------+

 <R> :Reset Settings.
 <S> :Confirm and Save Settings.

<ESC>:Go to Previous Menu.
```

Example 1: FX port 1 Tx off if any port 2, 3, 4 Rx loss:
keyin 1,2,3 and keyin 0 to change 'and' to 'or'

Example 2: FX port 1 Tx off if all ports 2, 3, 4 Rx loss
keyin 1,2,3 and leave Port 1 as 'And'

Example 3: FX port 1 Tx off if port 3 Rx loss
keyin 2 (only one selected so logic doesn't care)

After setting up the matrix, you must press <S> to **Confirm and Save** the settings.

3.8 SNMP Configuration

3.8.1 General

The Simple Network Management Protocol (**SNMP**) is one of many protocols in the Internet Protocol (IP) suite. SNMP is the protocol recommended specifically for the exchange of management information between hosts residing on IP networks. Network management allows you to monitor and control network devices remotely using conventional computer network technology.

The SNMP management functions of the **1000EAS** are provided by an internal SNMP agent, which utilizes communication over IP networks. The SNMP agent is compliant with the SNMPv1 and V2C standards. SNMP communications use the User Datagram Protocol (UDP). UDP is a connectionless transport protocol, part of the TCP/IP suite. The SNMP application uses an asynchronous command/response polling protocol and operates at the OSI Layer 7 (Layer 7 is the Application Layer. Other IP applications that operate at this layer are FTP, Telnet, HTTP, SMTP, etc.). All management traffic is initiated by the SNMP-based network management station. Only the addressed managed entity (agent) answers the polling of the management station (except for trap messages).

3.8.2 SNMP Operations

The SNMP protocol includes four types of operations:

getRequest	Command for retrieving specific value of an "instance" from the managed node. The managed node responds with a getResponse message.
getNextRequest	Command for retrieving sequentially specific management information from the managed node. The managed node responds with a getResponse message.
getBulkRequest	Command for retrieving a block of management information from the managed node. The managed node responds with a getResponse message. getBulkRequest was introduced in SNMPv2.
setRequest	Command for manipulating the value of an "instance" within the managed node. The managed node responds with a getResponse message.
trap	Management message carrying unsolicited information on extraordinary events (that is, events which occurred not in response to a management operation) reported by the managed node.

3.8.3 The Management Information Base

The management information base (MIB) includes a collection of managed objects. Managed objects are defined as parameters that can be managed, such as specific information on device configuring or on performance statistics values.

The MIB includes the definitions of relevant managed objects (MIB variables) for the specific node. Various MIB's can be defined for various management purposes, types of equipment, etc. The management data itself is a collection of integer, string and MIB address variables that contain all the information necessary to manage the node.

A leaf object's definition includes the range of instances (values) and the "access" rights:

Read-only	Instances of an object can be read, but cannot be set.
Read-write	Instances of an object can be read or set.
Write-only	Instances of an object can be set, but cannot be read.
Not accessible	Instances of an object cannot be read, nor set.

3.8.4 MIB Structure

The MIB has an inverted tree-like structure (root over leaves), with each definition of a managed instance forming one leaf, located at the end of a branch of that tree. Each "leaf" in the MIB is reached by a unique path. By numbering the branching points, starting with the top, each leaf can be uniquely defined by a sequence of numbers. The formal description of the managed objects and the MIB structure is provided in a special standardized format, called Abstract Syntax Notation 1, or **ASN.1** (pronounced A-S-N dot one).

Since the general collection of MIB's can also be organized in a similar structure, under the supervision of the Internet Activities Board (IAB), any parameter included in a MIB that is recognized by the IAB is uniquely defined.

To provide the flexibility necessary in a global structure, MIB's are classified in various classes (branches), one of them being the experimental branch, another being the management (mgmt) branch, and yet another the group of private (enterprise-specific) branches. Under the private enterprise-specific branch of MIB's, each enterprise (manufacturer) can be assigned a number, which is its enterprise number. The assigned number designates the top of an enterprise-specific sub-tree of non-standard MIB's.

Enterprise-specific MIB's are published and distributed by their creators, who are responsible for their contents. The MIB supported by the **FRM220-1000EAS** SNMP Agent follows RFC 1213 (MIB-2 standard).

3.8.5 SNMP Communities

To enable the delimitation of management domains, SNMP uses "communities". Each community is identified by a name, which is an alphanumeric string of up to 255 characters defined by the user. Any SNMP entity (this term includes both managed nodes and management stations) is assigned by its user a community name. In parallel, the user defines for each SNMP entity a list of the communities which are authorized to communicate with it, and the access rights associated with each community (this is the SNMP community name table of the entity).

In general, SNMP agents support two types of access rights:

Read-only	the SNMP agent accepts and processes only SNMP getRequest and getNextRequest commands from management stations which have a read-only community name.
Read-write	the SNMP agent accepts and processes all the SNMP commands received from a management station with a read-write community name. SNMP agents are usually configured to send traps to management stations having read-write communities.

3.8.6 Configuring the SNMP Agent

The agent for the **1000EAS** is embedded. From the Main Menu page, select <M> **SNMP Manager**. Manager configuration is required to tell the agent (the SNMP) who has authority to access the SNMP via "Get" commands (read) or "Set" commands (write) and where to send "trap" messages (unsolicited messages that are usually generated by alarms in the **1000EAS**).

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< SNMP Manager Configuration Setup >>
   Manager's IP        Community String Access
   ================== ================ ==========
#1 ---                 ---              ---
#2 ---                 ---              ---
#3 ---                 ---              ---
#4 ---                 ---              ---
#5 ---                 ---              ---
#6 ---                 ---              ---
#7 ---                 ---              ---
#8 ---                 ---              ---

<1>~<8>:Edit Manager #1 to #8 Settings.
  <D>  :Delete All Settings.
  <N>  :Go to Trap Configuration Menu.

 <ESC> :Go to Previous Menu.
```

The manager configuration has the ability to setup access for up to eight (8) different management workstations. The community strings act like passwords in dealing with the device via SNMP protocol. By assigning a manager's IP address, a community string, and assigning read/write or read only authority, an administrator can be granted control access to the **1000EAS**.

```
          ******************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ******************************************
<< SNMP Manager Configuration Setup >>
   Manager's IP        Community String Access
   ================== ================ ==========
#1 59.125.162.247      secret           read-write
#2 59.125.162.242      public           read-only
#3 ---                 ---              ---
#4 ---                 ---              ---
#5 ---                 ---              ---
#6 ---                 ---              ---
#7 ---                 ---              ---
#8 ---                 ---              ---

<1>~<8>:Edit Manager #1 to #8 Settings.
  <D>  :Delete All Settings.
  <N>  :Go to Trap Configuration Menu.

 <ESC> :Go to Previous Menu.
```

Note that in the above example, the management workstation with IP address 59.125.162.247 and using the community string 'secret', has full read and write access. The management station at 59.125.162.242 has read only privileges when using the community string 'public'.

3.8.7 Configuring SNMP Traps

A **trap** is a type of **PDU** (Protocol Data Unit) used to report an alert or other asynchronous event about a managed subsystem. Traps are unsolicited messages sent by the agent to the network management software. They may be a system specifically generated message or they could be programmed through the Alarm Management, see section 3.3.2.

The only configuration done here for traps is to enter the trap destination IP address. From the SNMP Manager menu, select <N> (Go to Trap Configuration Menu).

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ********************************************
<< Trap Configuration Setup >>
   Trap Receiver IP Community String
   ================ ================
#1 ---              ---
#2 ---              ---
#3 ---              ---
#4 ---              ---
#5 ---              ---
#6 ---              ---
#7 ---              ---
#8 ---              ---

<1>~<8>:Edit Trap Receiver #1 to #8 Settings.
  <D>  :Delete All Settings.

 <ESC> :Go to Manager Configuration Menu.
```

This SNMP agent supports up to eight (8) SNMP trap receivers that can be entered into this configuration menu.

```
          ********************************************
          ***    CTC UNION TECHNOLOGIES CO., LTD.   ***
          ***      FRM220-1000EAS     Ver:3.240     ***
          ********************************************
<< Trap Configuration Setup >>
   Trap Receiver IP Community String
   ================ ================
#1 59.125.162.247   secret
#2 ---              ---
#3 ---              ---
#4 ---              ---
#5 ---              ---
#6 ---              ---
#7 ---              ---
#8 ---              ---

<1>~<8>:Edit Trap Receiver #1 to #8 Settings.
  <D>  :Delete All Settings.

 <ESC> :Go to Manager Configuration Menu.
```

In the above example, the SNMP network manager at 59.125.162.247 IP will receive traps.

Chapter 4 Provisioning Via Web Based Management

4.1 Introduction

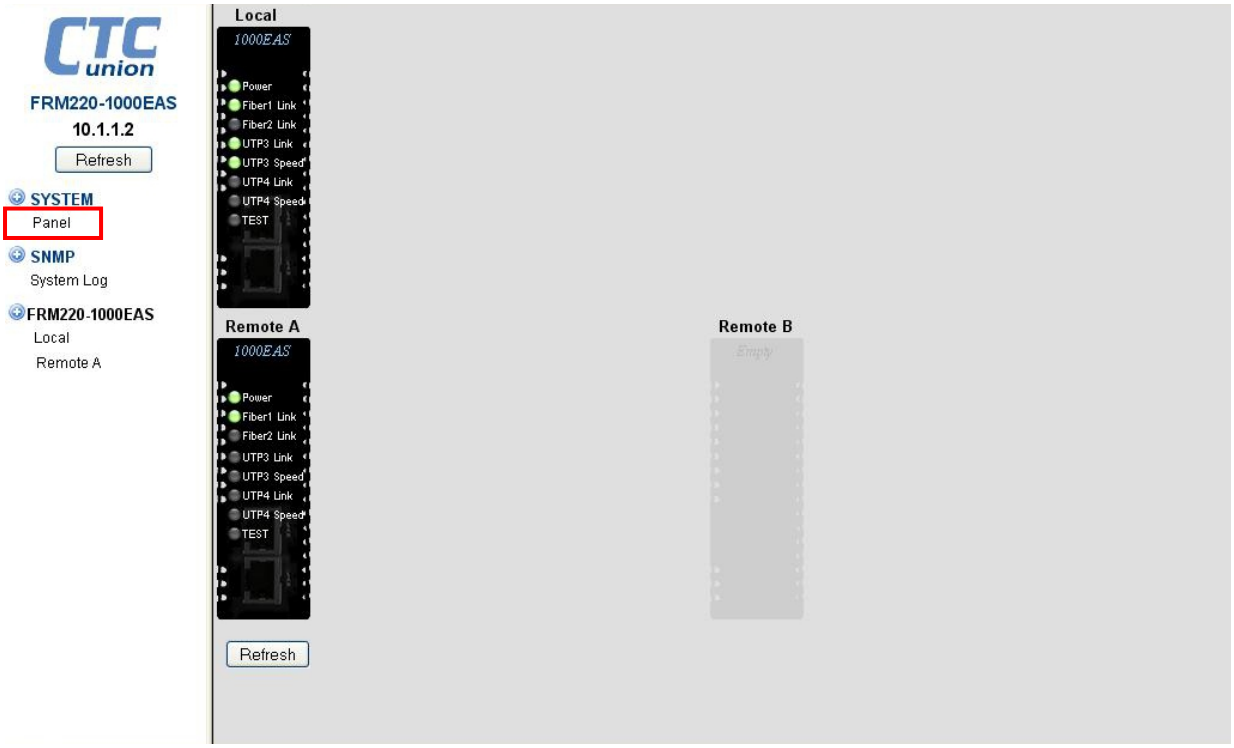
In an effort to make Networking devices easier to configure, many devices can now be configured via a Web Page, which should be familiar to all Internet users.

The web page is accessed by the Default IP Address of the device from a Web Browser such as Internet Explorer or Firefox in the following way:

10.1.1.1/ (Assuming the Default IP Address is 10.1.1.1)

Before accessing this device by web browser, the IP address must be known or it must be reset or changed to be used on the desired network. Please refer to Chapter 1, section 1.7 for the factory reset procedure and to Chapter 2, section 3.2 for Telnet login and section 3.3 for System Configuration settings.

4.2 Web Main Page



The **1000EAS** has two fiber and two copper ports. Because it uses 802.3ah OAM on the fiber links for remote in-band management, it is able to see up to two (2) remote devices. The 'Remote A' device is connected to this unit's FIBER 1 port. If another **1000EAS** series is connected to FIBER 2 port, then it will show up on this page as 'Remote B'. Each unit is shown with the exact LED status in real time.

The areas that support click on this screen are the graphic images themselves (directly into those units) and from the Menu item window on the left part of the screen,

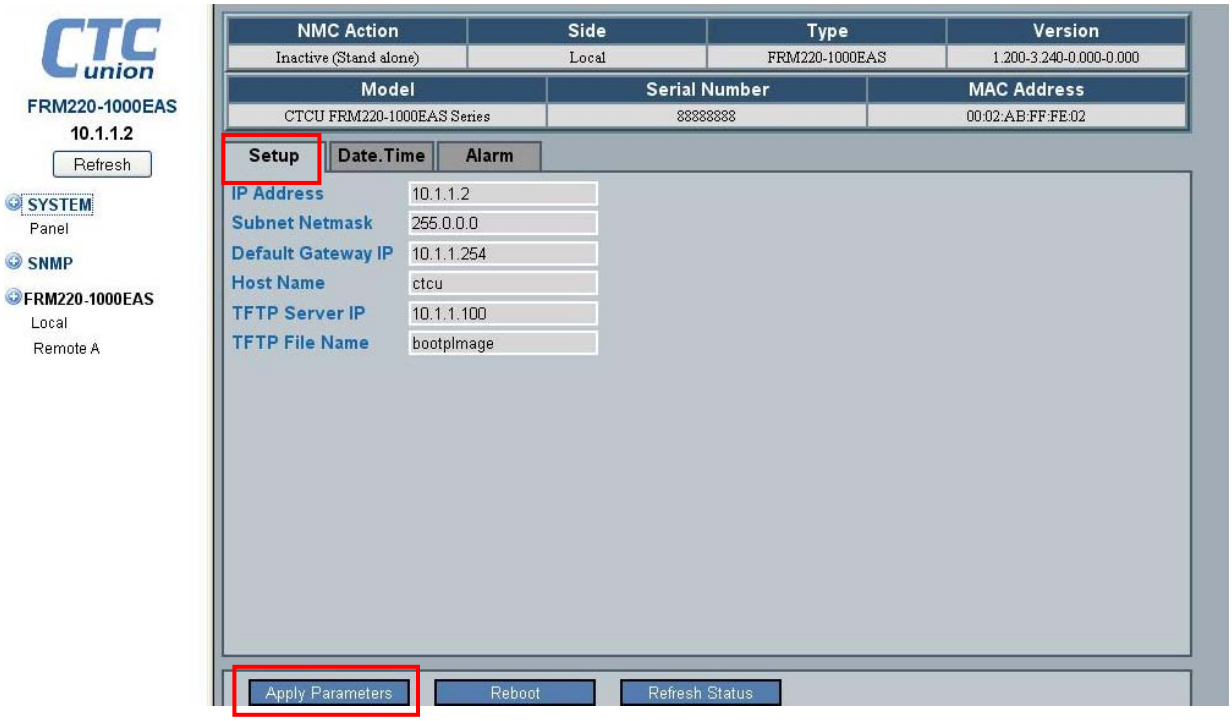
1. System – The device's network settings, date & time and the alarm configurations are set here.
2. SNMP – The allowed SNMP managers, community strings and Trap Managers are set here. There is also a 'System Log' which can be viewed by selecting System Log under the SNMP main menu item.
3. The actual **FRM220-1000EAS** units, local, Remote A, and Remote B can be entered for configuration with these items.

4.3 System

The following page is an example of the 'System' screen of the 1000EAS. There are three 'Tabs' for different setting windows.

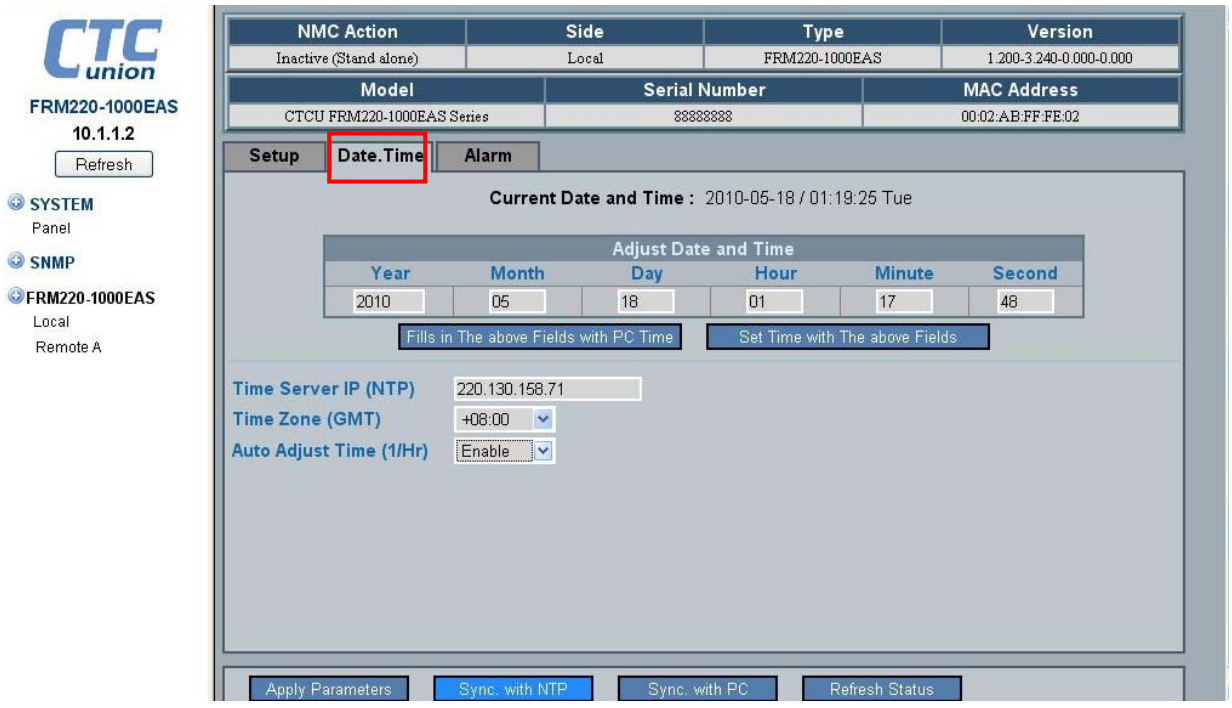
4.3.1 Setup

The 'Setup' tab contains the networking settings for IP address, subnet mask, default gateway, hostname, TFTP server IP and image upgrade filename. After filling in, click the 'Apply Parameters' button.



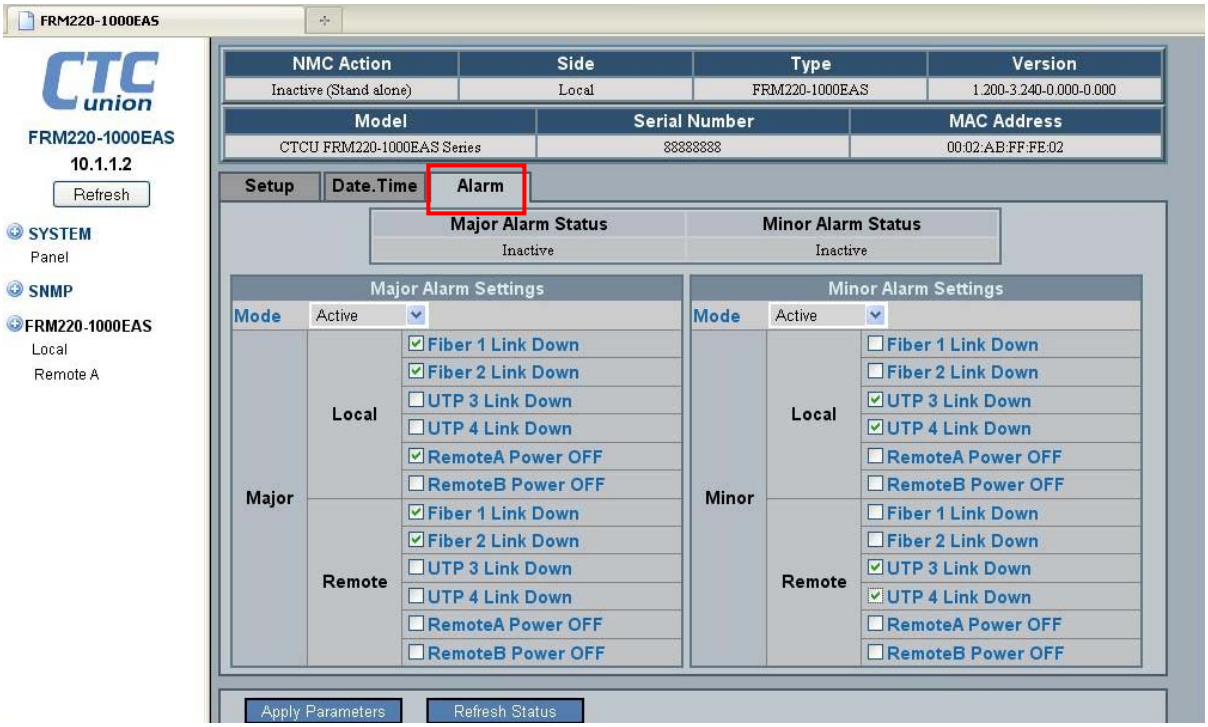
4.3.2 Date & Time

The Date & Time tab provide real time, from PC clock, or SNTP network time settings.



4.3.3 Alarm Setting

The alarm settings here are used to generate SNMP traps for any of the Major and Minor conditions via simple to click 'checkboxes'. In the example below, Major alarms are sent for Fiber link loss or Remote power failure while Minor alarms are sent for UTP link loss.

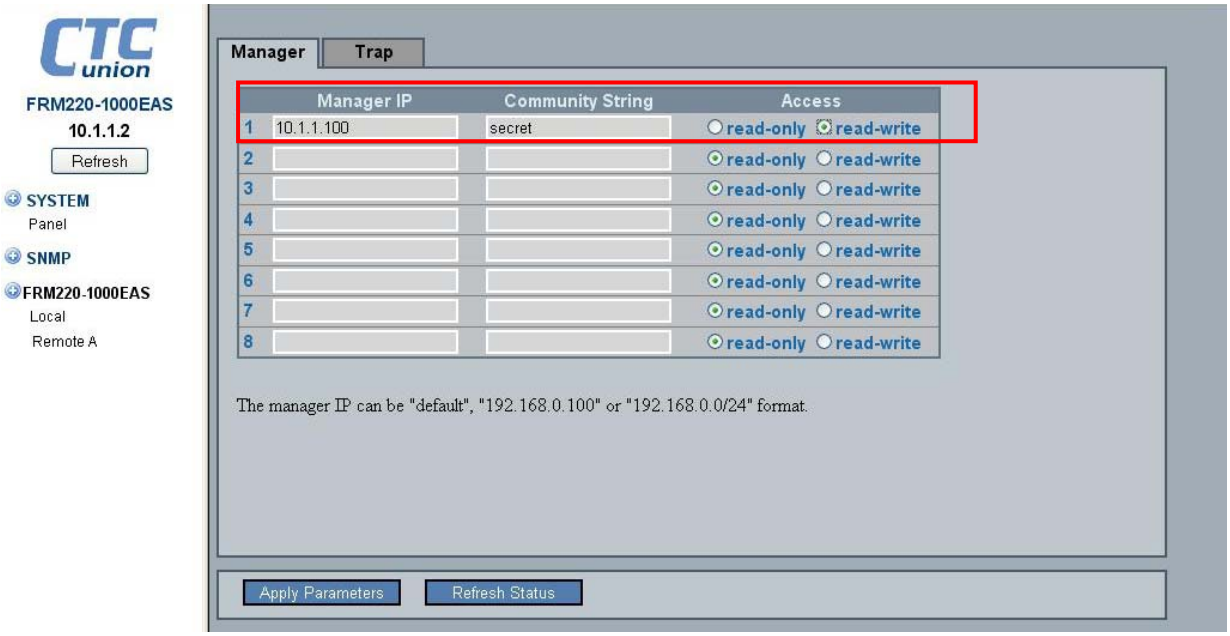


4.4 SNMP

The SNMP setting window is divided into two tabs, one for Manager Configuration and one for Trap Configuration.

4.4.1 Manager

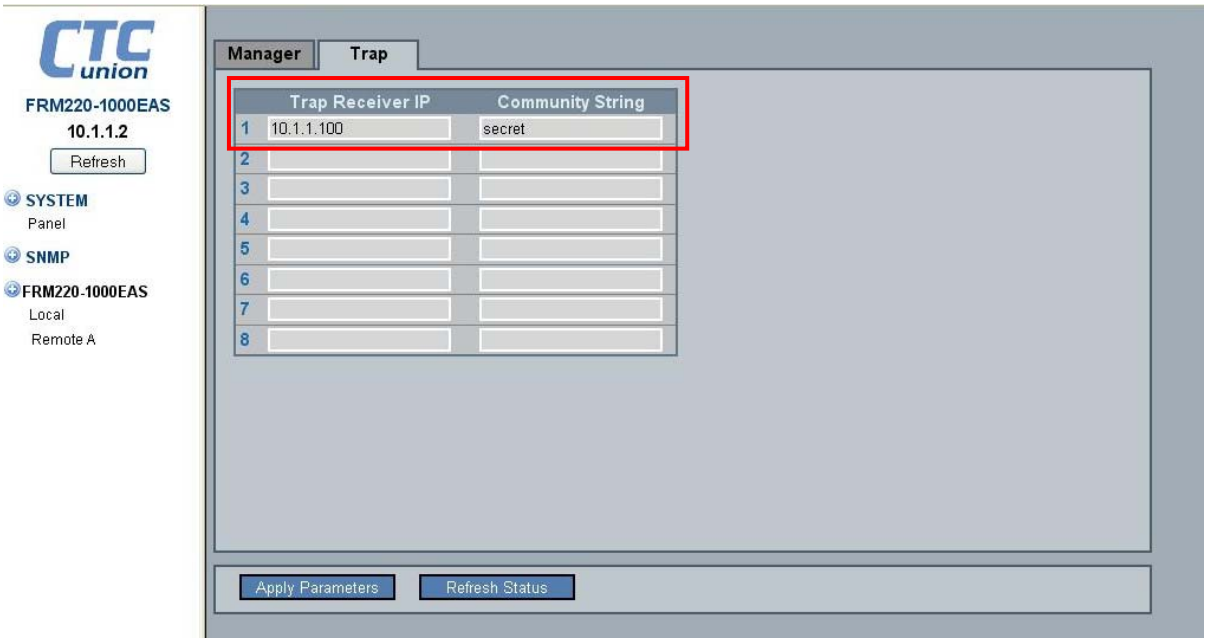
By setting the manager's IP and community string in this window, authority is granted to the network manager. There are eight (8) locations for entering manager information.



Manager at 10.1.1.100 with string 'secret' is granted 'read-write' access to SNMP.

4.4.2 Trap

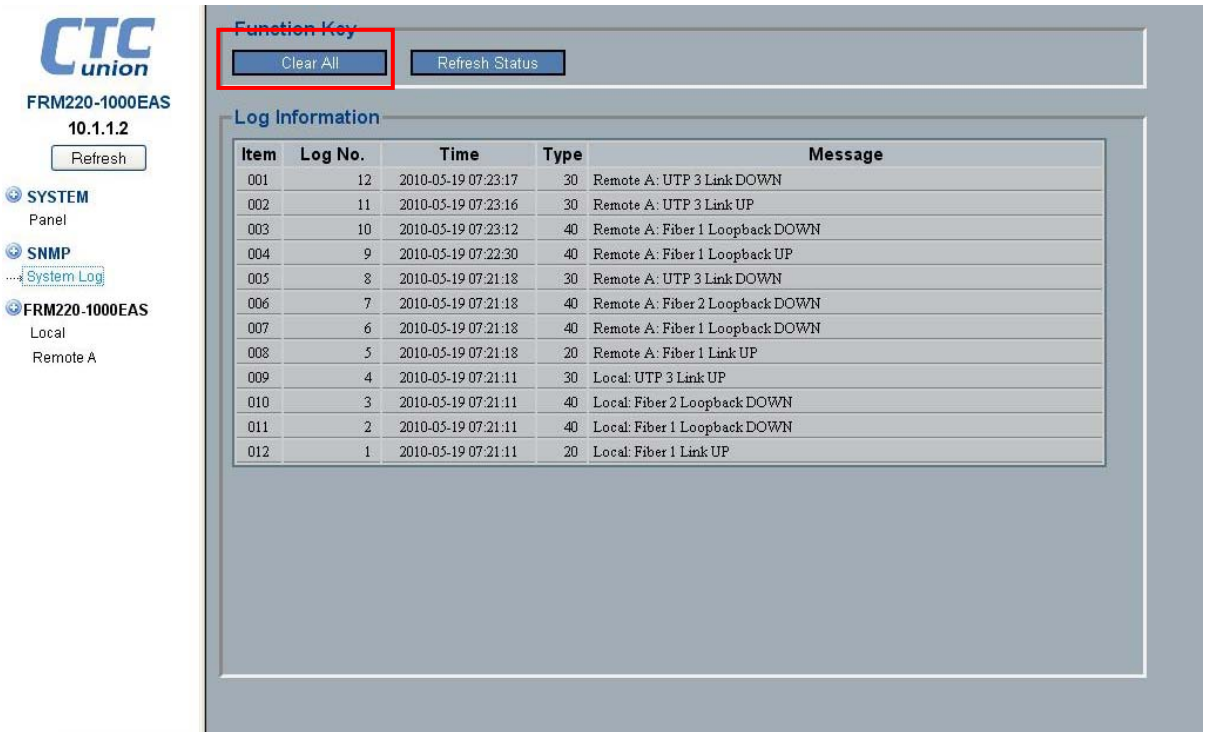
Traps are unsolicited messages issued by the SNMP agent that typically indicate some alarm condition has occurred. The Trap managers (those who receive the traps) are configured here.



SNMP manager at 10.1.1.100 receives traps with community 'secret'.

4.4.3 System Log

During the current up time of the 1000EAS converter, as system log is maintained and can be viewed through the web interface. This is a first-in first-out log that holds up to 100 entries. The log will display information such as user logins from Web or from Telnet and any of the Major and Minor alarms as programmed in the alarm setting page (refer to 4.3.3).

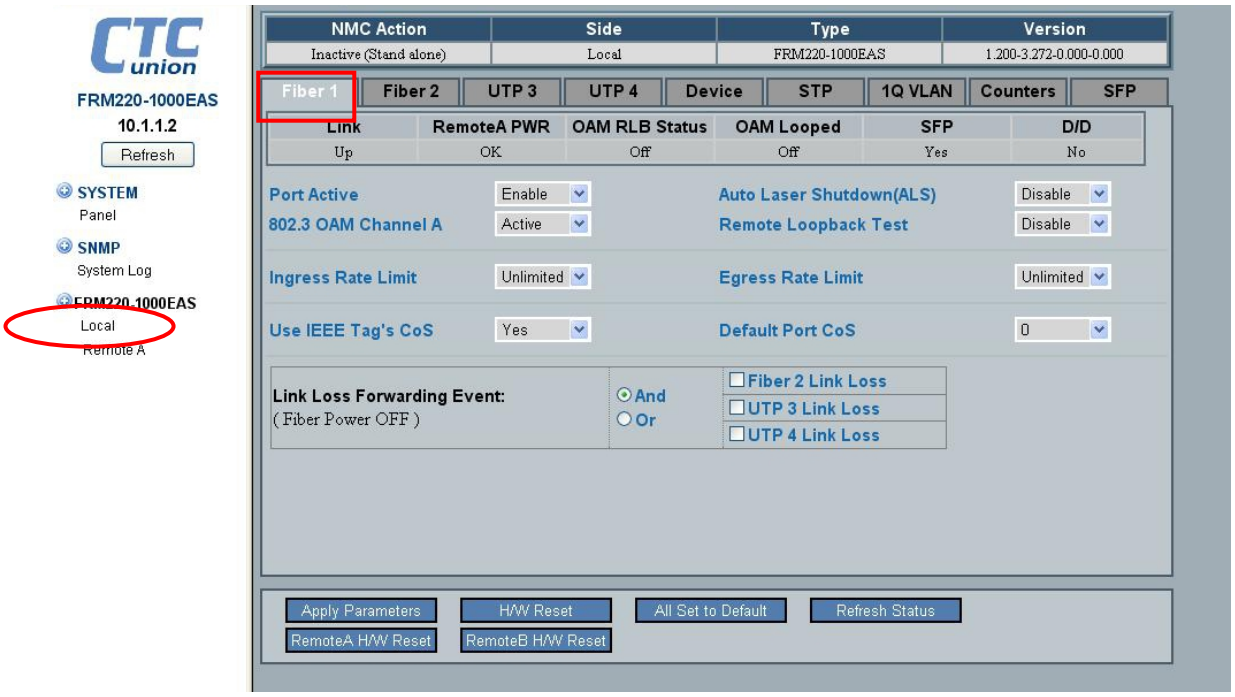

FRM220-1000EAS
10.1.1.2
Refresh
SYSTEM
Panel
SNMP
System Log
FRM220-1000EAS
Local
Remote A
Function Key
Clear All
Refresh Status
Log Information
Item Log No. Time Type Message
001 12 2010-05-19 07:23:17 30 Remote A: UTP 3 Link DOWN
002 11 2010-05-19 07:23:16 30 Remote A: UTP 3 Link UP
003 10 2010-05-19 07:23:12 40 Remote A: Fiber 1 Loopback DOWN
004 9 2010-05-19 07:22:30 40 Remote A: Fiber 1 Loopback UP
005 8 2010-05-19 07:21:18 30 Remote A: UTP 3 Link DOWN
006 7 2010-05-19 07:21:18 40 Remote A: Fiber 2 Loopback DOWN
007 6 2010-05-19 07:21:18 40 Remote A: Fiber 1 Loopback DOWN
008 5 2010-05-19 07:21:18 20 Remote A: Fiber 1 Link UP
009 4 2010-05-19 07:21:11 30 Local: UTP 3 Link UP
010 3 2010-05-19 07:21:11 40 Local: Fiber 2 Loopback DOWN
011 2 2010-05-19 07:21:11 40 Local: Fiber 1 Loopback DOWN
012 1 2010-05-19 07:21:11 20 Local: Fiber 1 Link UP

The "Clear All" button can be used to clear out all the log entries.

4.5 Local Unit Configuration

4.5.1 Fiber 1

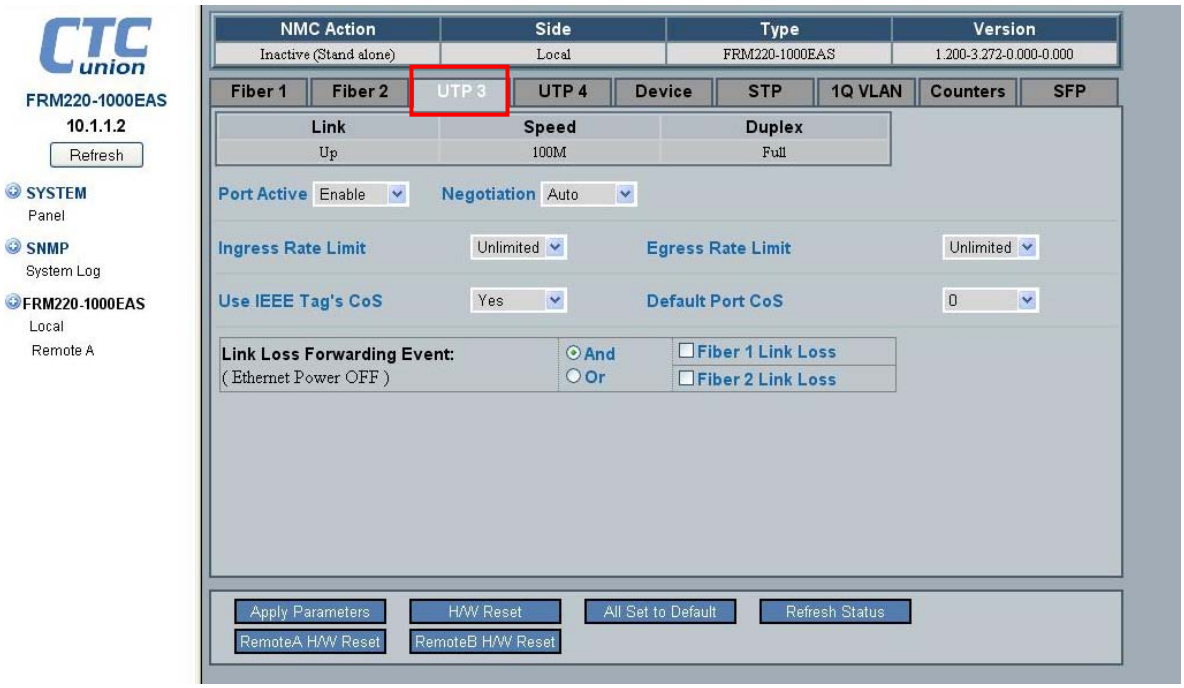
This window tab will show current status and provide settings for the first fiber port.



Refer to Chapter 3 section 3.3.6 and 3.3.7 for the meaning of these parameter settings. The setting method for Fiber 2 is identical to that of Fiber 1.

4.5.2 UTP 3

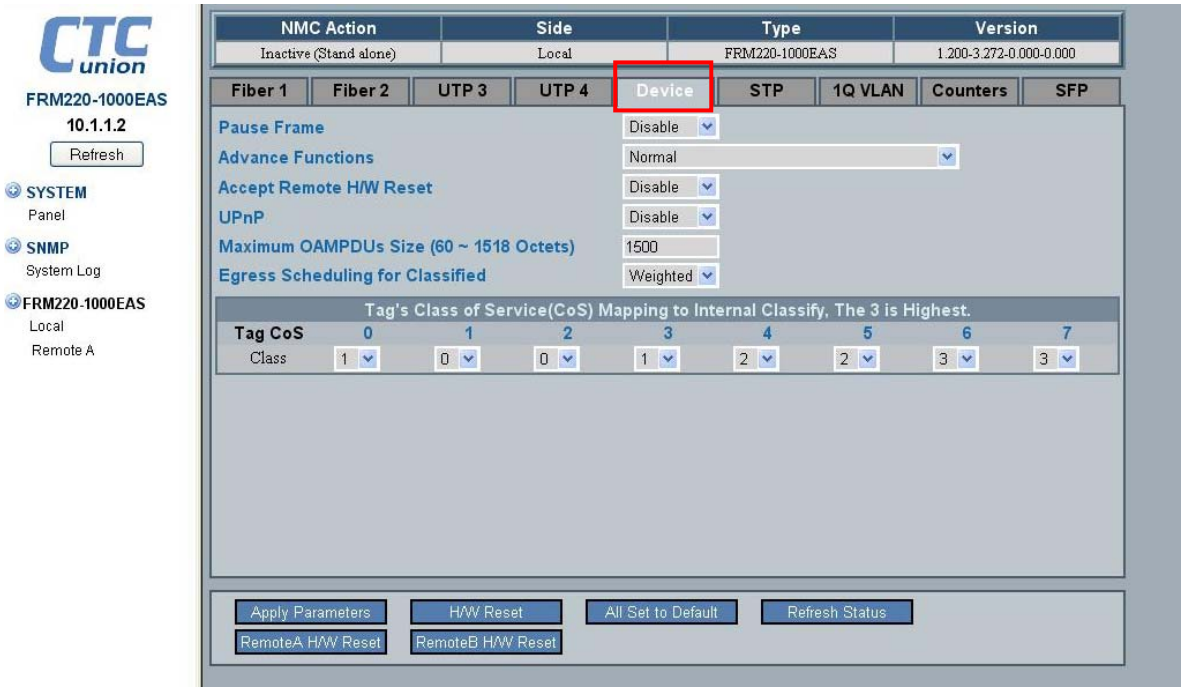
This window tab will show current status and provide settings for the first UTP port.



Refer to Chapter 3 section 3.3.9 for the meaning of these parameter settings. The setting method for UTP 4 is identical to that of UTP 3.

4.5.3 Device Status and Configuration

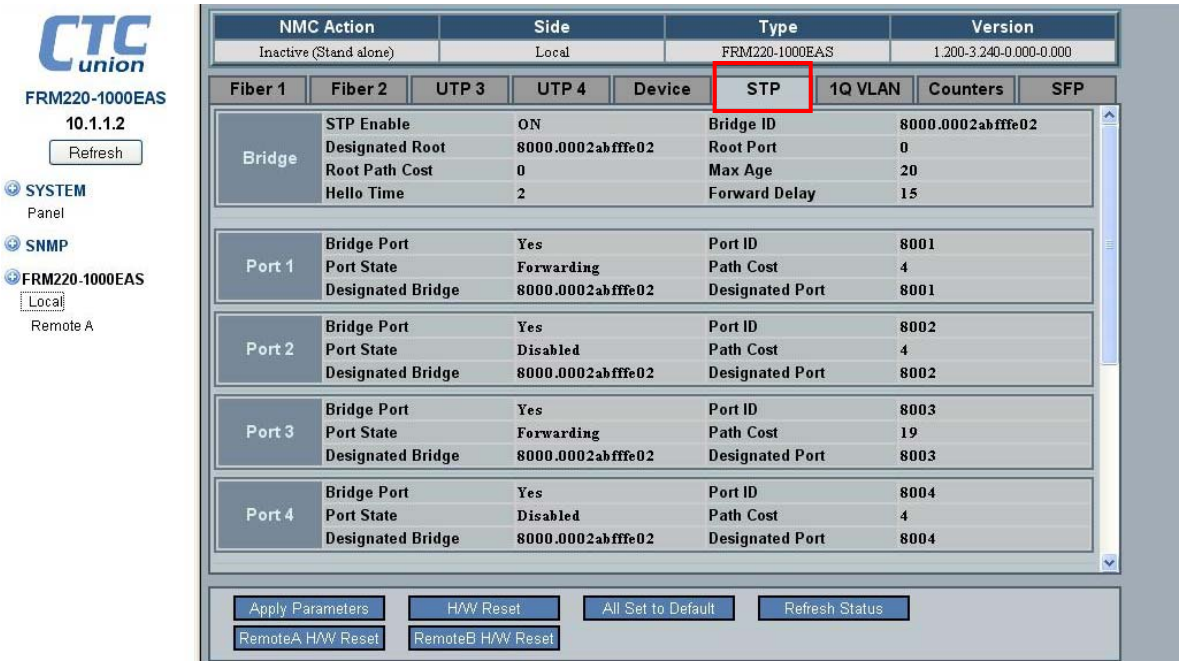
The settings here are described in Chapter 3 section 3.4. Please refer to that section.



The 'Advanced Functions' for this device are detailed in Chapter 3 section 3.5. Please refer to that section. Refer to section 3.5.9 for settings of CoS.

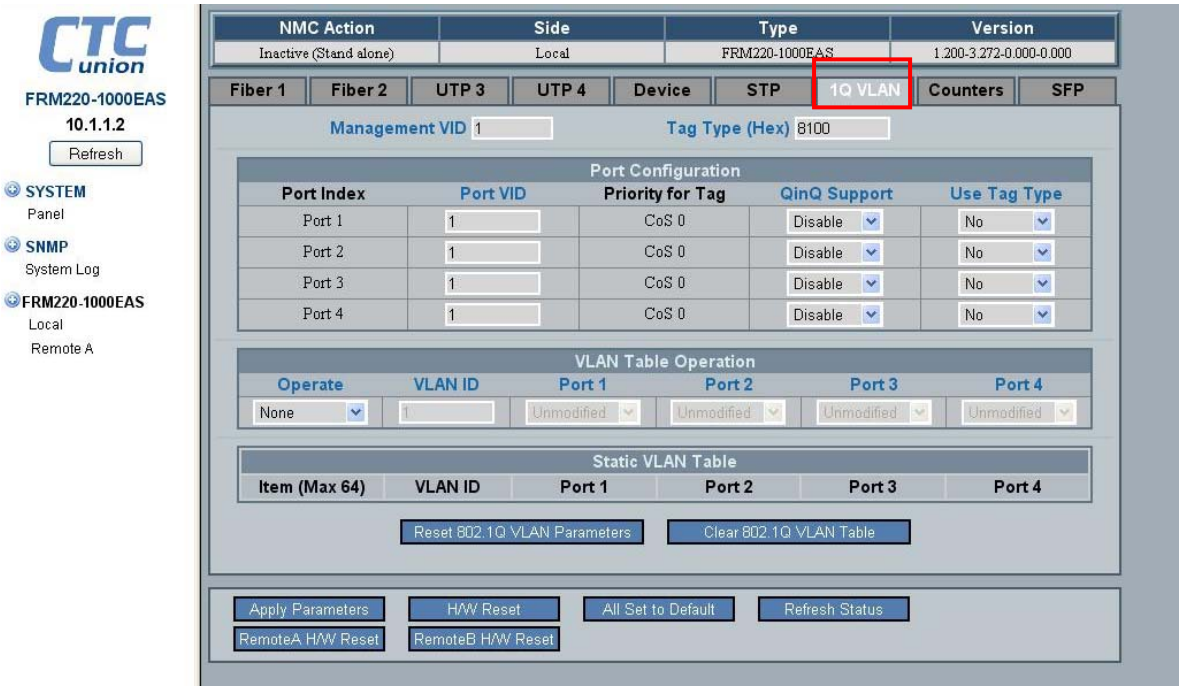
4.5.4 Spanning Tree Protocol

Please refer to Chapter 3, section 3.5.8 for a description of and operation of STP in this device.



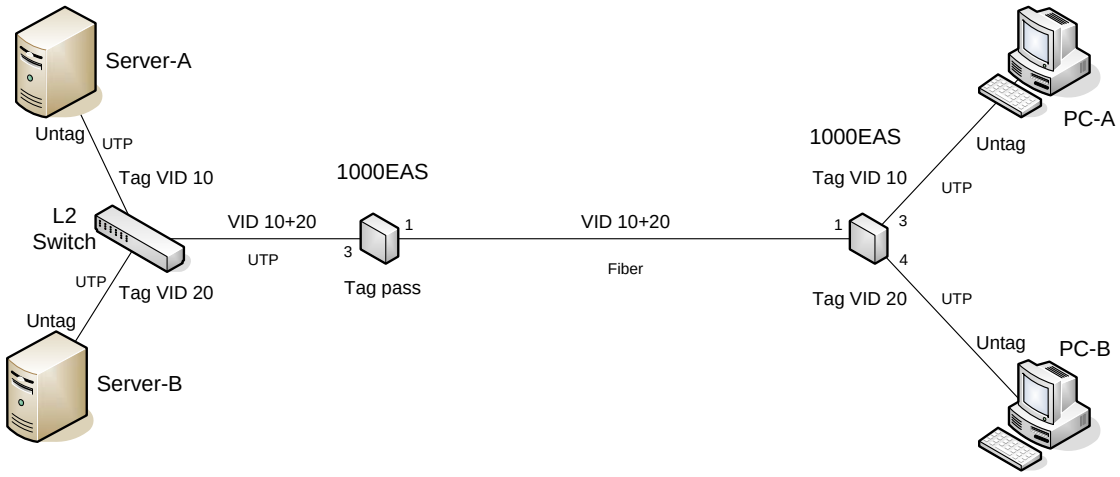
4.5.5 Static 802.1Q VLAN

Please refer to Chapter 3, section 3.5.5 for a description of and operation of Static VLAN feature in this device and to 3.5.9 for Class of Service settings.

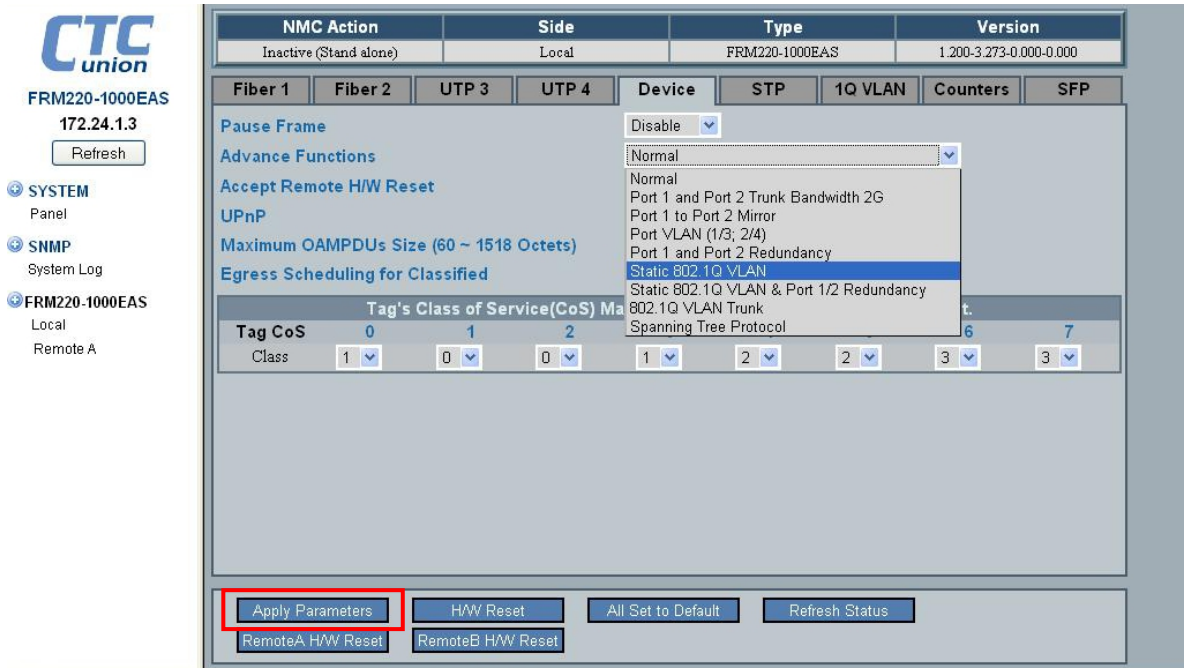


Static VLAN Example

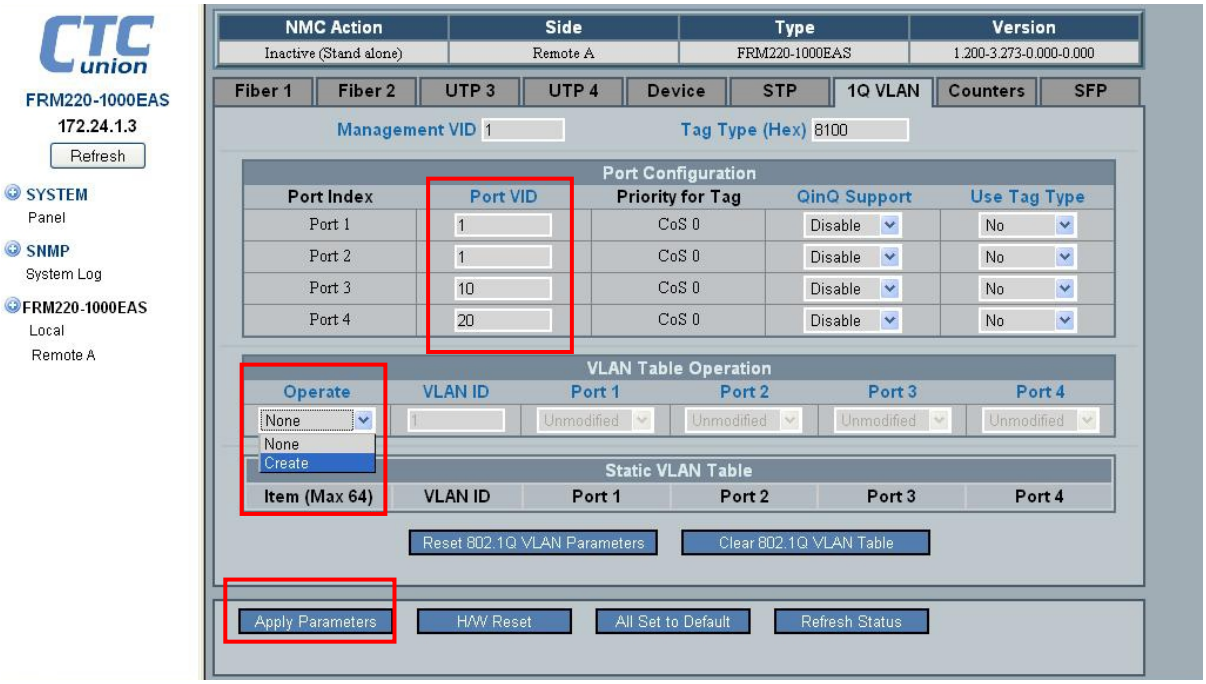
This static VLAN application was used in Chapter 3 section 3.5.5. Here we will use the web based interface to do the settings rather than the Telnet menu system. This should help the end user to better understand the setting methodology using the friendlier web interface.



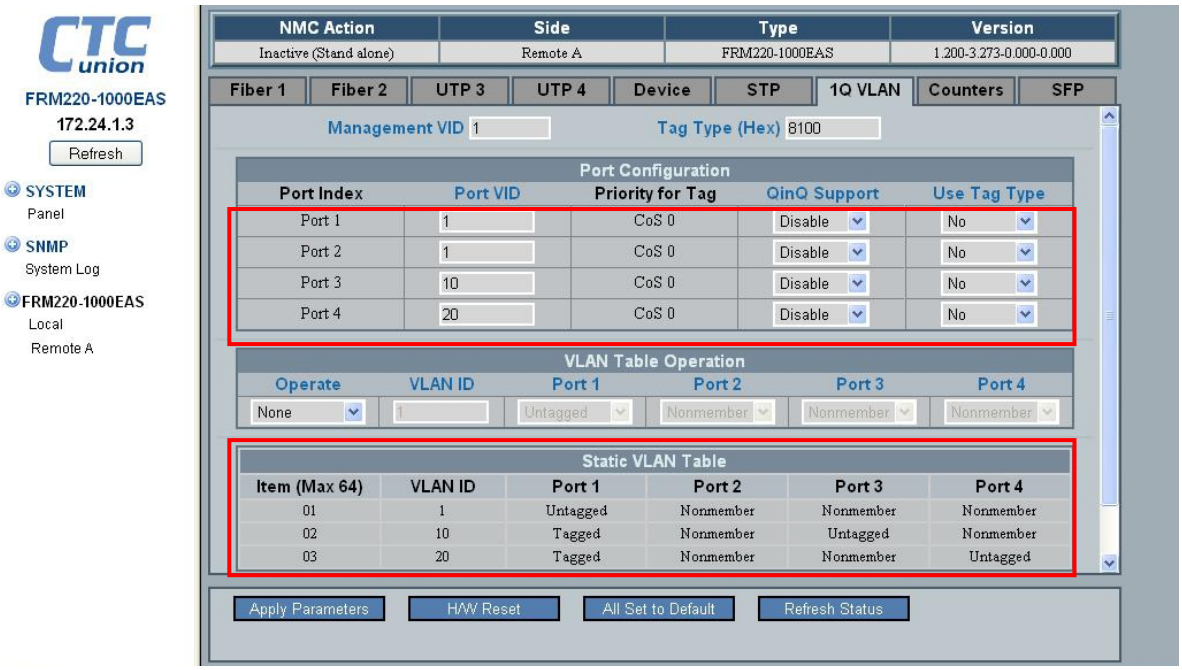
Step 1. Under the Device, Advanced Functions, enable the Static 802.1Q VLAN from the pull-down. Click 'Apply Parameters'.



Step 2. Setup the VID for 1, 10, and 20 for the fiber and two UTP ports. Then, from the 'Operate' pull-down, select 'Create' and one by one setup the VID1, VID10 and VID20 static VLANs.



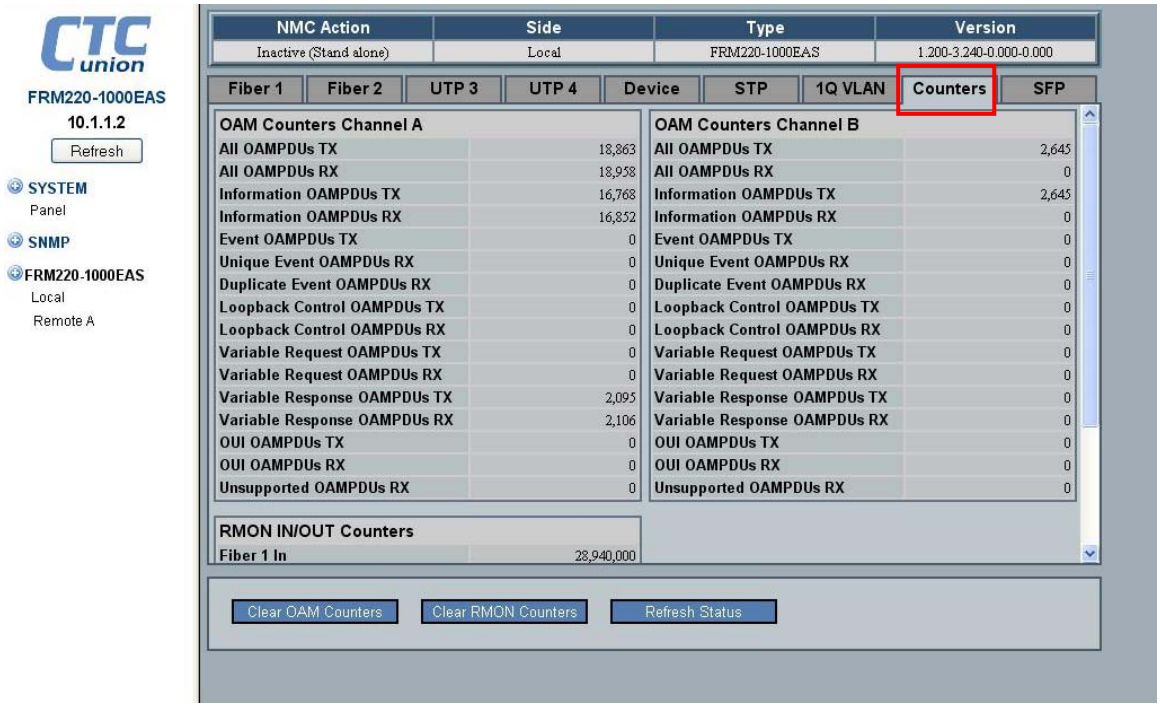
Step 3. For each created VID click 'Apply Parameters'. When finished, the screen will look like the following.



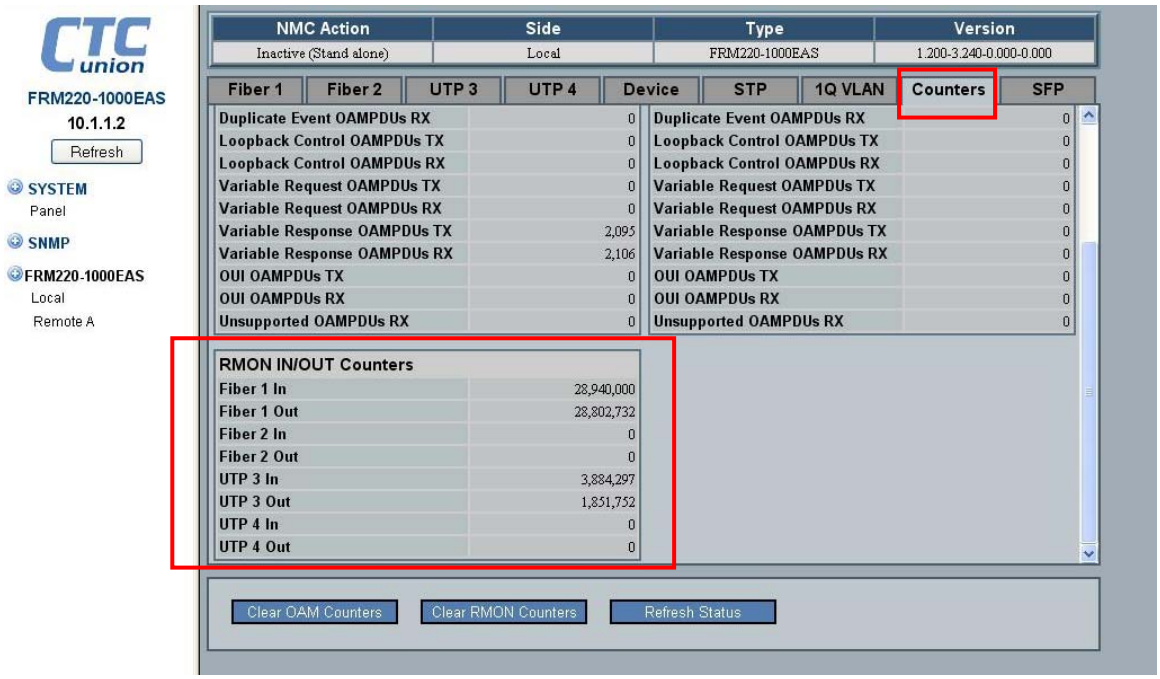
Some Tagging definitions:
Tagged: This means that packets that egress the assigned port will have the packets tagged with the VID assigned to that port.
Untagged: This means that any packets that egress the assigned port will have all tag information removed.
Non-member: When a port is not a member of a VID, packets tagged with that VID will not be allowed to egress that port. (i.e. they will be dropped)

4.5.6 Counters

There are counters for OAM packets and counters for RMON data bytes. They can be viewed under the 'Counter' screens.



The OAM counters are available for each fiber port. In this example the Fiber 2 channel is not connected, so there are no received packets.

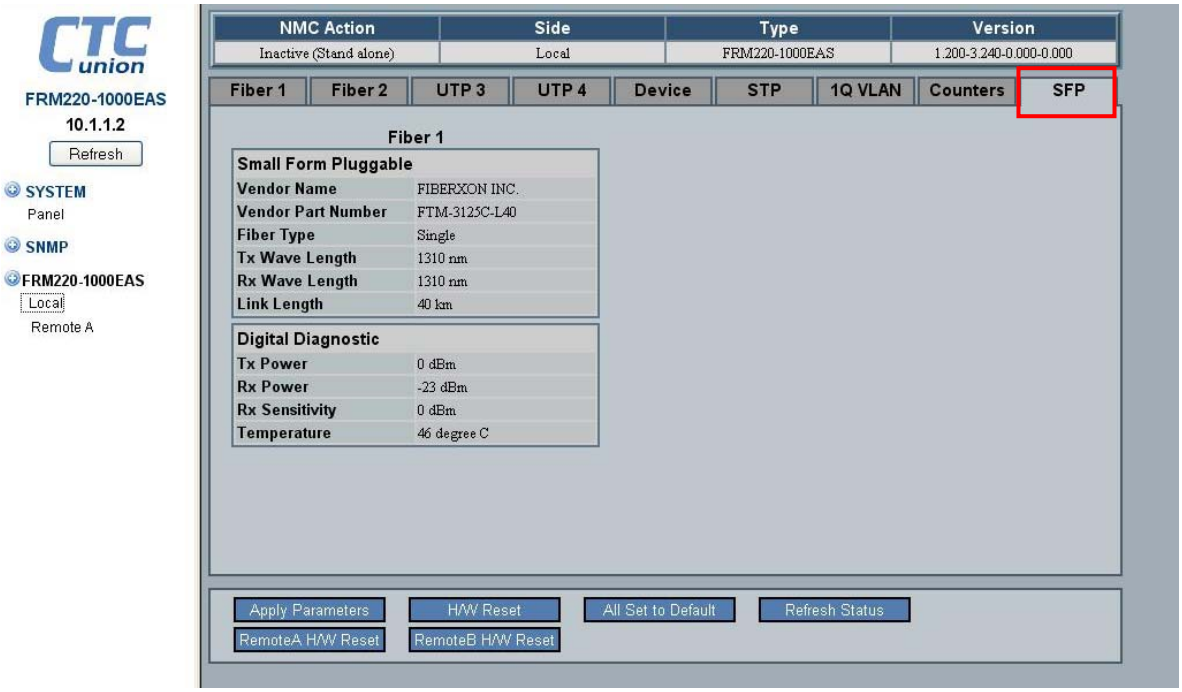


The RMON in/out counters show the received and transmitted bytes for each of the interfaces on the **1000EAS**.

To clear the counters, click either the 'Clear OAM Counters' or 'Clear RMON Counters' button.

4.5.7 SFP

Modern optical SFP transceivers support digital diagnostics monitoring (DDM) functions according to the industry-standard SFF-8472. This optional feature in SFP is also known as digital optical monitoring (DOM) and gives the end user the ability to monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, etc. DDM is not available in every SFP, so if the inserted SFP does not support DD, there will be no view for it. However, every SFP should be able to view the manufacturer name, part number, fiber type and link length. To view the SFP particulars, click the 'SFP' tab.



4.6 Remote Configuration

By utilizing 802.3ah proprietary OAM packets, the 1000EAS is able to view the status and manage the remote device without using Internet Protocol. All settings are done the same as the local device.

CTC union

www.ctcu.com

T +886-2 2659-1021 F +886-2 2659-0237 E info@ctcu.com

ISO 9001 Quality System Certified CTC Union Technologies Co.,LTD.

All trademarks are the property of their repective owners. Technical information in this document is subject to change without notice.